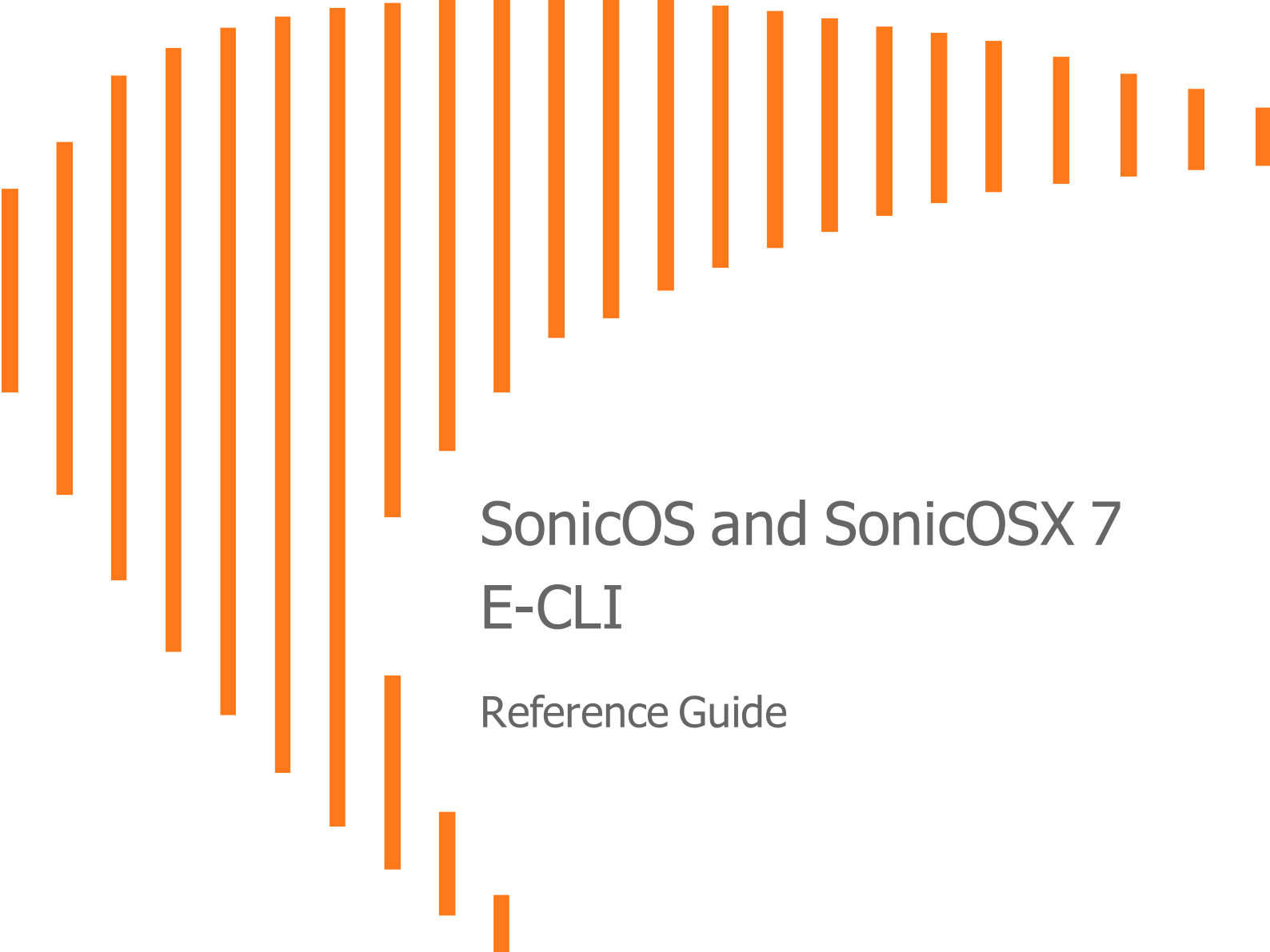




SonicOS and SonicOSX 7 E-CLI

Reference Guide

SONICWALL[®]

Contents

Introduction	3
Text Conventions	3
CLI Prompt Specification	4
Input Data Format Specification	4
Editing and Completion Features	4
Command Hierarchy	5
Passwords	7
Factory Reset to Defaults	7
Logging into the SonicOS/X E-CLI	7
Configuring the SonicWall Network Security Appliance	8
Configuring Features using the CLI on a Serial Connection via the Console Port	8
Configuring Features using the CLI in an SSH Management Session via Ethernet	10
E-CLI-Supported Features	10
About SafeMode	11
Example of Configuring a Site-to-Site VPN Using E-CLI	11
CLI Access	12
Configuring a Site-to-Site VPN	12
Viewing a VPN Configuration	14
Interfaces	17
User Interfaces	17
Advantages of CLI	17
Using a Terminal Emulator or SSH Client	18
Configuring New SonicWall Appliances With CLI	18
Routing & OSPF Configuration	19
To Configure Routing	19
To Configure OSPF	19
Advanced Routing with ZebOS CLI	20
Using OSPFv3	20
Top Level and System Commands	22
E-CLI Commands	24
ecli_help	25
SonicWall Support	2273
About This Document	2273

Introduction

① **NOTE:** References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.

The SonicWall SonicOS and SonicOSX Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall network security appliances without using the SonicOS/X web-based management user interface (UI).

You can use the CLI commands individually on the command line, or in scripts for automating configuration tasks. In addition, with SonicWall E-CLI, you can copy the output of a show command and post it back as a CLI command at the prompt. This feature gives the interface even greater speed and flexibility.

This document contains an introduction to E-CLI and a categorized list of the E-CLI commands for the SonicOS/X firmware. Each command is described, and where appropriate, an example of usage is included. Some commands, conventions, and connections are different for different SonicWall appliances.

Topics:

- [Text Conventions](#)
- [CLI Prompt Specification](#)
- [Input Data Format Specification](#)
- [Editing and Completion Features](#)
- [Command Hierarchy](#)
- [Passwords](#)
- [Factory Reset to Defaults](#)
- [Logging into the SonicOS/X E-CLI](#)
- [Configuring the SonicWall Network Security Appliance](#)
- [Example of Configuring a Site-to-Site VPN Using E-CLI](#)

Text Conventions

Bold text indicates a command executed by interacting with the user interface.

Italic text indicates the first occurrence of a new term, as well as a book title, and also emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets ("**< >**") are required information.

Items within square brackets ("**[]**") are optional information.

Items separated by a "pipe" ("**|**") are options. You can select any of them.

NOTE: Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line, with no carriage returns except at the end of the complete command.

CLI Prompt Specification

A user-selected firewall name, chosen through the SonicOS/X web UI on the **System > Administration** screen, is subsequently used in the prompts throughout the CLI, rather than a generic product name.

This allows the administrator to more easily identify which firewall is currently being managed, and to identify which firewalls are used for which departments in a business structure. For example, the administrator might name firewalls with names like Marketing, Tech Pubs, Engineering, and Testing.

The format is:

"currentusername@firewallname".

If no firewall name is configured, the default is the serial number or MAC address of the device, resulting in a prompt such as:

```
admin@C0EAE45998CC>
```

Input Data Format Specification

The table that follows describes the data formats acceptable for most CLI commands. H represents one or more hexadecimal digit (0-9 and A-F). D represents one or more decimal digit.

INPUT DATA FORMATS

Data	Data Format
MAC Address	HH:HH:HH:HH:HH:HH
MAC Address	HHHHHHHHHHHHHH
MAC Address	HH-HH-HH-HH-HH-HH
IPv4 Address	d.d.d.d
IPv6 Address	HHHH:HHHH:HHHH:HHHH: HHHH:HHHH:HHHH:HHHH
Integer Values	D
Integer Values	0xHH

Editing and Completion Features

You can use individual keys and control-key combinations to assist you with the CLI commands in the SonicOS/X interface. The table below describes the key and control-key combination functions.

① | **NOTE:** Some of the functions could be different on the E-CLI for your appliance.

KEY REFERENCE

Key(s)	Function
Tab with letters	Completes the word, or gives options if there are several
Tab alone	Displays possible commands
?	Displays possible commands with descriptions
Ctrl+A	Moves cursor to the beginning of the command line
Ctrl+B	Moves cursor to the previous character
Ctrl+C	Exits the Quick Start Wizard at any time
Ctrl+E	Moves cursor to the end of the command line
Ctrl+F	Moves cursor to the next character
Ctrl+K	Erases characters from the cursor to the end of the line
Ctrl+N	Displays the next command in the command history
Ctrl+P	Displays the previous command in the command history
Ctrl+W	Erases the previous word
Left Arrow	Moves cursor to the previous character
Right Arrow	Moves cursor to the next character
Up Arrow	Displays the previous command in the command history
Down Arrow	Displays the next command in the command history

The **Tab** key can also be used to finish a command if the command is uniquely identified by user input.

```
user@devicename ect. > show lo[TAB]
```

displays as:

```
user@devicename ect. > show logs
```

In addition, commands can be abbreviated, as long as the partial commands are unique. The following text:

```
user@devicename ect. > sho inter
```

is an acceptable abbreviation for, and displays as:

```
user@devicename ect. > show interface <interface name>
```

Command Hierarchy

The CLI allows you to control the hardware and firmware of the appliance through a discreet mode and submode system. The commands for the appliance fit into the logical hierarchy of this mode and submode system.

To configure items in a submode, you must activate the submode by entering a command in the mode above it.

For example, to set the default LAN interface speed or duplex, type:

```
configure
```

```
interface x0
```

link-speed auto-negotiate.

exit/end

commit

There must be an explicit “commit” command to make the configuration take effect. It is possible to commit within a submode, but this only submits the changes within the submode. To commit all of the changes, commit from the config mode.

Together with the commit and submode concept, there are two other commands that also depend on the mode. These are “show current-config” and “show pending config”.

Access these commands from:

(edit-interface[X0])# show

current-config Show current configuration.

pending-config Show pending configuration.

E.g.

config(C0EAE45998CC)# interface X0

(edit-interface[X0])# show current-config

ip-assignment LAN static

ip 192.168.168.168

netmask 255.255.255.0

no gateway

exit

comment "Default LAN"

...

(edit-interface[X0])# comment test

(edit-interface[X0])# show pending-config

ip-assignment LAN static

exit

comment test

(edit-interface[X0])# commit

% Applying changes...

% Status returned processing command:

commit

% Changes made.

(edit-interface[X0])# show current-config

```
ip-assignment LAN static
  ip 192.168.168.168
  netmask 255.255.255.0
  no gateway
  exit
```

comment test

Passwords

The SonicOS/X CLI currently uses the administrator's password to obtain access to the network. SonicWall network security appliances are shipped with a default password. The user should set a secure password for accessing the appliance and configuring it over a network.

In addition to the full admin user, E-CLI also supports limited/readonly admin/guest.

Factory Reset to Defaults

If, at some point, you are unable to connect to your device over the network, follow the steps below during a serial configuration session to reset the device to factory defaults.

1. Go to Configure mode.
2. Run "restore-defaults".

 **CAUTION:** The "restore" command erases all the settings on the appliance, leaving it in a factory default state.

Logging into the SonicOS/X E-CLI

When the connection is established, log into the security appliance:

1. At the User Name prompt, enter the Admin username. Only the admin user can login from the CLI. The default Admin username is admin. The user should change the username from the default.
2. At the Password prompt, enter the Admin password. The CLI prompt specification is `admin@my570TZ>`. The format is `user@firewallname`.
3. When an invalid or mismatched username/password are entered, the system returns to the User Name prompt, and a error message states "CLI administrator login denied due to bad credentials." There is no lockout on the CLI.

Configuring the SonicWall Network Security Appliance

You can configure the SonicWall network security appliance using one of the three methods described below. These descriptions are examples of configurations for accessing the Enterprise Command Line Interface. Your equipment may require a different configuration.

- [Configuring Features using the CLI on a Serial Connection via the Console Port](#)
- [Configuring Features using the CLI in an SSH Management Session via Ethernet](#)
- [E-CLI-Supported Features](#)
- [About SafeMode](#)

① **NOTE:** To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find a suitable, free, terminal emulator to download from the Internet.

Configuring Features using the CLI on a Serial Connection via the Console Port

You do not need to assign an IP address to the firewall to use the CLI on a serial connection to the Console port.

① **NOTE:** The default terminal settings on the firewall are 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

To configure features using the CLI on a serial connection via the console port:

1. Attach an RJ-45 to DB-9 serial cable to the appliance port marked CONSOLE. Attach the other end of the cable to a serial port on the configuring computer.

Console Port

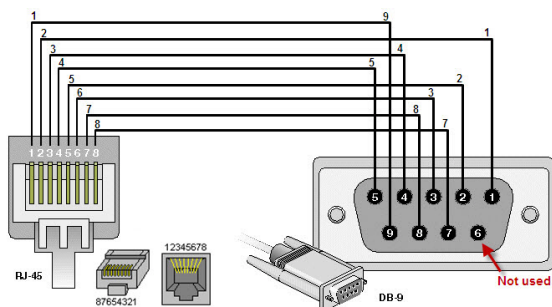
Provides access to the SonicOS Command Line Interface (CLI) via the DB9 -> RJ45 cable



2. The RJ-45 to DB-9 serial cable pin assignments are as follows:

RJ-45 Connector	DB-9 Connector
Pin 1	Pin 9
Pin 2	Pin 1
Pin 3	Pin 4
Pin 4	Pin 5
Pin 5	Pin 2
Pin 6	Pin 3
Pin 7	Pin 8
Pin 8	Pin 7
Pin 9	Pin 6 – not used

The RJ-45 to DB-9 serial cable pin diagram is shown below:



3. Launch a terminal emulation application that communicates with the serial port connected to the appliance. Use these settings:
 - 115,200 baud
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control
4. Press **Enter/Return**. Initial information is displayed followed by a **Device Name> Prompt**.

Configuring Features using the CLI in an SSH Management Session via Ethernet

You can use an SSH client to access the CLI by connecting to the appliance with an Ethernet cable. This option is useful for customers who do not have access to an RJ-45 to DB-9 serial cable for the Console port on the firewall.

To use SSH management, you must assign an IP address to X0 (LAN) or X1 (WAN), or use the default LAN IP address of 192.168.168.168.

To configure features using the CLI in an SSH management session via Ethernet:

1. Attach an Ethernet cable to the interface port marked X0. Attach the other end of the Ethernet cable to an Ethernet port on the configuring computer.
2. Launch a terminal emulation application or SSH client that communicates via Ethernet.
3. In the emulation application, enter the IP destination address for the X0 interface, and enter 22 as the port number.
4. Select SSH as the connection type and open a connection.

E-CLI-Supported Features

You can manage the appliance securely from your web browser using HTTPS, by connecting to either the LAN or WAN IP address of the appliance directly or over the network. Refer to the *SonicOS/X Administration Guide* for complete information about the SonicOS/X management User Interface (web UI).

Many of the same tasks can also be performed using E-CLI. The following features can be configured and managed from the SonicOS/X CLI interface:

Category	Features
Dashboard	All features
3G/4G/Modem	All features
System	All features
SonicPoint	All features
Rules and Policies	All features
Firewall Settings	All features
DPI-SSL/DPI-SSH	All features
Anti-Spam	All features
Users	All features
Security Services	All features
WWAN	All features
AppFlow	All features
Log	All features

About SafeMode

SafeMode is a limited web management interface that provides a way to upload firmware from your computer and reboot the appliance. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** screen.

There is an E-CLI command “safemode” that restarts the firewall in safemode.

For more information on SafeMode for your firewall, refer to the *Getting Started Guide* for your appliance.

① | **NOTE:** The CLI commands are not available in SafeMode.

Example of Configuring a Site-to-Site VPN Using E-CLI

This section describes how to create a VPN policy using CLI. You can configure all of the parameters using CLI, and enable the VPN without using the web management interface.

① | **NOTE:** In this example, the VPN policy on the other end has already been created.

Topics:

- [CLI Access](#)
- [Configuring a Site-to-Site VPN](#)
- [Viewing a VPN Configuration](#)

CLI Access

As in other Command Line Interfaces, such as UNIX Shell or Cisco IOS, auto-complete is provided, so you only have to type the first few letters of a command. The rest is automatically completed for you by the system.

1. Use a DB9 to RJ45 connector to connect the serial port of your PC to the console port of the firewall.
2. Use a terminal emulator program such as PuTTY or Tera Term (downloaded from the Internet) with the following set parameters:
 - 115,200 baud
 - 8 bits
 - No parity
 - 1 stop bit
 - No flow control
3. You might need to click return several times to get to a command prompt. In this example, the command prompt is:
TZ570>
4. When you need to make a configuration change, you must be in configure mode. To enter configure mode, type configure.
TZ570> configure
5. The command prompt changes and adds the word config to distinguish it from normal mode. In configure mode, you can configure all the settings, enable and disable the VPNs, and configure the firewall.
(config[TZ570])>

Configuring a Site-to-Site VPN

This is an example of configuring a Site-to-Site VPN using CLI:

```
config(C0EAE45998CC)# address-object ipv4 "Office LAN"
(add-ipv4-address-object[Office LAN])# zone VPN
(add-ipv4-address-object[Office LAN])# network 192.168.15.0 255.255.255.0
(add-ipv4-address-object[Office LAN])# exit
config(C0EAE45998CC)# commit
% Applying changes...
% Status returned processing command:
    commit
% Changes made.
show address-object ipv4 "Office LAN"
vpn policy site-to-site testS2S
```



```
enable
gateway primary 2.2.2.2

auth-method shared-secret
    shared-secret 11111111
    exit

network local any
network remote name "Office LAN"
proposal ike exchange ikev2
proposal ike encryption aes-128
proposal ike authentication sha-1
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-128
proposal ipsec authentication sha-1
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
no netbios
anti-replay
no wxa-group
no multicast
no management https
no management ssh
no management snmp
no keep-alive
no allow-sonicpointn-layer3
no user-login http
no user-login https
no default-lan-gateway
bound-to zone WAN
no suppress-trigger-packet
no accept-hash
no send-hash
no suppress-auto-add-rule
no apply-nat
exit

commit

show vpn policy ipv4 site-to-site testS2S
```

Viewing a VPN Configuration

To view a list of all the configured VPN policies:

1. Type the command show vpn policy. The output is similar to the following:

```
(config[TZ570])> show vpn policy
Policy: WAN GroupVPN (Disabled)
Key Mode: Pre-shared
Pre Shared Secret: DE65AD2228EED75A
Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users
Client:
Cache XAUTH Settings: Never
Virtual Adapter Settings: None
Allow Connections To: Split Tunnels
Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF
Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: sonicwall
IKE ID:
Local: IP Address
Peer: IP Address
Network:
Local: LAN Primary Subnet
Remote: OfficeLAN

Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
```

Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

2. To view the configuration for a specific policy, specify the policy name in double quotes.

For example:

```
(config[TZ570])> show vpn policy "OfficeVPN"
```

The output is similar to the following:

Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: sonicwall
IKE ID:
Local: IP Address
Peer: IP Address
Network:
Local: LAN Primary Subnet
Remote: OfficeLAN
Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

3. Type the command show vpn sa [name] to see the active SA:

```
(config[TZ570])> show vpn sa "OfficeVPN"
```

Policy: OfficeVPN
IKE SAs
GW: 10.50.31.150:500 --> 10.50.31.104:500
Main Mode, 3DES SHA, DH Group 2, Responder
Cookie: 0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)
Lifetime: 28800 seconds (28783 seconds remaining)
IPsec SAs
GW: 10.50.31.150:500 --> 10.50.31.104:500

(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)
ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2
Lifetime: 28800 seconds (28783 seconds remaining)

Interfaces

Topics:

- [User Interfaces](#)
- [Advantages of CLI](#)
- [Using a Terminal Emulator or SSH Client](#)
- [Configuring New SonicWall Appliances With CLI](#)

User Interfaces

- The Graphic User Interface (GUI) is the one casual computer users are the most familiar with. It consists of moving users through screens in order to accomplish tasks. Users are led through a series of screens with prompts to click in certain boxes or other areas of the screen, usually with a minimum of keyboard work. A GUI is usually user-friendly, and conversational.
- The Application Program Interface (API) is a set of routines, tools, and protocols for building software applications. The API is like a translating tool, allowing two different languages, two different instruction sets, to work together to accomplish tasks. Along with other software components, APIs are used to program GUIs. APIs are intended to be only machine-readable, since they are programmed into the applications.
- The Command Line Interface (CLI), on the other hand, is a direct human interface with the machine, but not through clicking boxes with the mouse. The CLI uses a series of commands with preset meanings, typed on the keyboard by the user at a prompt on the screen. The commands are then translated by the computer into various actions. E-CLI for SonicOS/X has the added advantage that “show” commands can be copied and pasted at the prompt, to speed up CLI configuration.

Advantages of CLI

Each interface has its advantages and disadvantages. More and more API providers are supporting a set of CLI commands alongside their API. A list of some of the benefits of the CLI is given below:

- A CLI is a human-readable interface that appeals to many developers' tastes. Most developers work from their favorite editor within the command line anyway, so CLI offers them the ability to stay where they are most comfortable and most productive.

- CLI can automate many tedious UI tasks. It offers powerful scripting capabilities, with the ability to connect many commands into one.
- This leads to a time savings for users. Once CLI commands have been scripted, they can accomplish many tasks with one user action.
- CLI commands can be used for advanced tasks in an interactive mode to debug or control an operating system. If launched from a command line shell, many normal programs allow further manipulation from within the CLI.
- Cloud computing is highly dependent on CLI, for interacting with virtual machines, spinning up instances, running applications in the cloud, arbitrating a virtual data center, and more. CLI is a developer's most effective method for initiating cloud transactions.
- Troubleshooting and testing of vulnerability would be impossible if not done from the command line. All remote access and file manipulation are done from the command line.

Using a Terminal Emulator or SSH Client

To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find a suitable, free, terminal emulator to download from the Internet.

Configuring New SonicWall Appliances With CLI

Many of the same tasks that can be done using the web-based SonicOS/X management interface, such as configuring a new appliance and backing up and restoring your appliance configuration, are available with expanded functionality from the CLI for administrators who prefer to work on the command line.

Routing & OSPF Configuration

This section explains how to configure Routing and OSPF (Open Shortest Path First). OSPF is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm, and therefore operates within a single autonomous system.

Topics:

- [To Configure Routing](#)
- [To Configure OSPF](#)
- [Advanced Routing with ZebOS CLI](#)

To Configure Routing

```
admin@my570TZ> config
config(my570TZ)# routing
(config-routing)#
```

To Configure OSPF

```
In routing mode,
(config-routing)# mode advanced
(config-routing)# ospf
ZebOS version 7.7.0 IPIRouter 7/2009
ARS OSPF>?
Exec commands:
```

clear	Reset functions
configure	Enter configuration mode
debug	Debugging functions (see also 'undebug')
exit	End current mode and down to previous mode
faults	Fault management command

help	Description of the interactive help system
no	Negate a command or set its defaults
show	Show command
terminal	Set terminal line parameters
undebg	Disable debugging functions (see also 'debug')
who	Display who is on vty
write	Write running configuration to memory, file or terminal

ARS OSPF>

Advanced Routing with ZebOS CLI

For advanced routing, SonicWall uses a third-party product, ZebOS CLI.

E-CLI provides the bridge to enter ZebOS CLI or to show the result from the ZebOS CLI as follows:

```
config(C0EAE45998CC)# routing
```

```
(config-routing)# os
```

```
ospf ospfv3
```

```
(config-routing)# ospf
```

```
ZebOS version 7.7.0 IPIRouter 7/2009
```

ARS OSPF>

Using OSPFv3

OSPFv3 is the OSPF version for IPv6.

```
(config-routing)# ospfv3
```

```
ZebOS version 7.7.0 IPIRouter 7/2009
```

ARS OSPFv3>?

Exec commands:

clear	Reset functions
configure	Enter configuration mode
debug	Debugging functions (see also 'undebg')
exit	End current mode and down to previous mode
faults	Fault management command
help	Description of the interactive help system
no	Negate a command or set its defaults
show	Show command

terminal	Set terminal line parameters
undebg	Disable debugging functions (see also 'debug')
who	Display who is on vty
write	Write running configuration to memory, file or terminal

Top Level and System Commands

This section provides some examples of Top Level and System CLI commands in SonicOS/X. They are entered at the `admin@COEAE45998CC>` prompt or `admin@COEAE45998CC> [Tab]`.

```
System Commands:
clear          Reset functions.
cli           CLI configuration.
diag          Diagnostic functions.
exit          Exit the current mode.
export        Export system status or configuration.
help          Display command help.
no            Negate a command or set its defaults.
show          Show system status or configuration.

Top Level Commands:
configure     Enter configuration mode.
geo-botnet-lookup Check GEO location and lookup BOTNET server.
kill-user     Log out users.
log-to-ftp    Log to FTP server.
mxlookup      MX lookup and banner check the specified domain name
              and SMTP port.
network-path  Find network path of the specified IP address.
nslookup      DNS lookup of the specified host.
ping          Ping the specified host.
pmtu-discovery Path MTU discovery to the specified host.
rbl-lookup    Lookup the specified realtime black list.
restart       Restart SonicOS.
reverse-lookup Resolve the specified reverse name.
safemode      Restart the device and enter safemode.
traceroute    Traceroute to the specified host.
unlock        Unlock a locked out IP address.
```

The following are entered with `admin@C0EAE45998CC> show`.

admin@C0EAE45998CC> show		
System Commands:		
cli	current-config	pending-config
Top Level Commands:		
access-rule	access-rules	action-object
action-objects	address-group	address-groups
address-object	address-objects	administration
anti-spyware	app-control	app-rules
appflow	arp	bandwidth-management
bandwidth-object	bandwidth-objects	botnet
capture-atp	certificate	certificates
checksum	client-enforcement	content-filter
dhcp-server	dns	dns-proxy
dns-security	dpi-ssh	dpi-ssl
dynamic-dns	email-object	email-objects
failover-lb	fips	firewall
firmware	gateway-antivirus	geo-ip
high-availability	icmp	interface
interfaces	intrusion-prevention	ip-helper
license	log	mac-ip-anti-spoof
match-object	match-objects	multicast
nat-policies	nat-policy	ndp
ndpp	network-monitor	packet-monitor
portshield-groups	qos-mapping	rbl
route-policies	route-policy	routing
schedule	schedules	sdwan
security-services	service-group	service-groups
service-object	service-objects	snmp
sonicpoint	ssh	ssl-control
ssl-vpn	status	switch
tcp	tech-support-report	time
tunnel-interface	tunnel-interfaces	udp
udpv6	user	version
virtual-assist	vlan-translation	vlan-translations
voip	vpn	web-proxy
zone	zones	

E-CLI Commands

The SonicOS/X E-CLI command list is provided in the following pages.

Click the command name to view its syntax and description.

Contents

- ecli/primitive.cdl
 - [clear](#)
 - [export](#)
 - [no](#)
 - [show](#)
 - [cancel](#)
 - [commit](#)
 - [commit-with-exit](#)
 - [end](#)
 - [end](#)
 - [exit](#)
 - [help](#)
- ecli/top.cdl
 - [configure](#)
- ecli/config.cdl
 - [no pending-config](#)
- ecli/debug.cdl
 - [dbg](#)
- ecli/cli.cdl
 - [cli idle-timeout default](#)
 - [cli screen width default](#)
 - [cli screen length default](#)
 - [cli show-unmodified default](#)
 - [no cli show-unmodified default](#)
 - [cli pager default](#)
 - [no cli pager default](#)
 - [cli interactive-prompts default](#)
 - [no cli interactive-prompts default](#)
 - [cli ftp user default](#)
 - [no cli ftp user default](#)
 - [cli ftp password default](#)
 - [no cli ftp password default](#)
 - [cli banner](#)
 - [no cli banner](#)
 - [clear screen](#)
 - [no cli history](#)
 - [cli history](#)
 - [cli format out](#)
 - [cli api-json](#)
 - [no cli api-json](#)
 - [cli idle-timeout session](#)
 - [cli screen width session](#)
 - [cli screen length session](#)
 - [cli show-unmodified session](#)
 - [no cli show-unmodified session](#)
 - [cli pager session](#)
 - [no cli pager session](#)
 - [cli interactive-prompts session](#)
 - [no cli interactive-prompts session](#)
 - [cli data-store index](#)
 - [no cli data-store index](#)
 - [cli ftp user session](#)
 - [no cli ftp user session](#)
 - [cli ftp password session](#)
 - [no cli ftp password session](#)
- ecli/config_show.cdl
 - [show current-config](#)
 - [show current-config](#)
 - [show pending-config](#)
- ecli/cli_show.cdl
 - [show cli](#)
- ecli/diag.cdl
 - [check-network](#)
 - [ping](#)
 - [traceroute](#)
 - [diag network-path](#)
 - [network-path](#)
 - [nslookup](#)
 - [diag reverse-lookup](#)
 - [reverse-lookup](#)
 - [diag rbl-lookup](#)
 - [rbl-lookup](#)
 - [diag mxlookup](#)
 - [mxlookup](#)
 - [diag geo-botnet-lookup](#)
 - [geo-botnet-lookup](#)
 - [pmtu-discovery](#)
 - [diag show abrentries](#)
 - [diag show processes](#)
 - [diag show process](#)
 - [diag show multicore](#)
 - [diag show build-info](#)
 - [diag show cpu](#)

- [diag show web-server](#)
- [diag show ssh-server](#)
- [diag show mem-pools](#)
- [diag show memory](#)
- [diag no show memory](#)
- [diag show timer-counters](#)
- [diag show wd-stats](#)
- [diag clear pp-stats](#)
- [diag show pp-stats](#)
- [diag clear active-utm](#)
- [diag show active-utm](#)
- [diag show debug interface](#)
- [diag test memory](#)
- [diag show alerts](#)
- [diag show log](#)
- [diag show drop-stats](#)
- [diag show pktio-nic](#)
- [diag show pktio-throughput-start](#)
- [diag show pktio-throughput-stop](#)
- [diag cli pager-test](#)
- [diag show switch port](#)
- [diag gen-coredump](#)
- [diag ipv6-check-network-settings](#)
- [diag cfs-lookup](#)
- [diag purge-coredump](#)
- [ecli/diag-advanced.cdl](#)
 - [diag advanced unified-policy-engine](#)
 - [no diag advanced unified-policy-engine](#)
 - [diag advanced arp](#)
 - [bridging](#)
 - [no bridging](#)
 - [open-arp-behavior](#)
 - [no open-arp-behavior](#)
 - [source-ip-validation](#)
 - [no source-ip-validation](#)
 - [only-unicast](#)
 - [no only-unicast](#)
 - [limit-nonresponsive](#)
 - [no limit-nonresponsive](#)
 - [redundant-ip-resolution-rate](#)
 - [no redundant-ip-resolution-rate](#)
 - [update-exist-arp](#)
 - [no update-exist-arp](#)
 - [bypass-for-l2bridge](#)
 - [no bypass-for-l2bridge](#)
 - [gratuitous-arp-compatibility](#)
 - [no gratuitous-arp-compatibility](#)
 - [secondary-subnet](#)
 - [no secondary-subnet](#)
 - [gratuitous-arp-limit](#)
 - [no gratuitous-arp-limit](#)
 - [system-broadcast](#)
 - [no system-broadcast](#)
 - [ignore-arps-with-primary-mac-from-other-if](#)
 - [no ignore-arps-with-primary-mac-from-other-if](#)
 - [display-mac-tracking](#)
 - [no display-mac-tracking](#)
 - [send system-arps](#)
 - [diag advanced network](#)
 - [flush-alternate-path-flows](#)
 - [no flush-alternate-path-flows](#)
 - [update-route-version](#)
 - [no update-route-version](#)
 - [tcp-packet-option-tagging](#)
 - [no tcp-packet-option-tagging](#)
 - [fix-malformed-tcp-headers](#)
 - [no fix-malformed-tcp-headers](#)
 - [sequence-number-randomization](#)
 - [no sequence-number-randomization](#)
 - [syn-validation](#)
 - [no syn-validation](#)
 - [clear ospf](#)
 - [debounce-interface-state-changes](#)
 - [no debounce-interface-state-changes](#)
 - [clear dont-fragment-bit](#)
 - [no clear dont-fragment-bit](#)
 - [smaller-first-fragment](#)
 - [no smaller-first-fragment](#)
 - [ipv6-small-fragment](#)
 - [no ipv6-small-fragment](#)
 - [override-mac](#)
 - [no override-mac](#)
 - [drop-record-route](#)
 - [no drop-record-route](#)
 - [dmz-icmp-redirect](#)
 - [no dmz-icmp-redirect](#)
 - [enforce-strict-tcp-compliance-rfc5961](#)
 - [no enforce-strict-tcp-compliance-rfc5961](#)
 - [learning-bridge-filter](#)
 - [no learning-bridge-filter](#)
 - [advertise-fqdn-route](#)

- [no advertise-fqdn-route](#)
- [generate-interface-default-route](#)
- [no generate-interface-default-route](#)
- [zebos-granular-debug](#)
- [no zebos-granular-debug](#)
- [diag advanced dns](#)
- [prefer-arpa](#)
- [no prefer-arpa](#)
- [stack-traffic-by-dp](#)
- [no stack-traffic-by-dp](#)
- [diag advanced dns-proxy](#)
- [request-size-percentage](#)
- [support-fragmentation](#)
- [no support-fragmentation](#)
- [server-failover-times](#)
- [no server-failover-times](#)
- [cache-lifetime](#)
- [no cache-lifetime](#)
- [dns-over-tcp](#)
- [no dns-over-tcp](#)
- [exclude-vpn-traffic](#)
- [no exclude-vpn-traffic](#)
- [diag advanced dns-security](#)
- [dns-tunnel-minimum-packet-number](#)
- [dns-tunnel-ratio-threshold](#)
- [dns-tunnel-number-threshold](#)
- [diag advanced dhcp](#)
- [network-pre-discovery](#)
- [no network-pre-discovery](#)
- [conflict-detect-period](#)
- [resources-to-discover](#)
- [conflicted-resource-timeout](#)
- [available-resource-timeout](#)
- [save leases](#)
- [dhcpnak](#)
- [no dhcpnak](#)
- [lease-database-refresh-interval](#)
- [lease-database-refresh-number](#)
- [use-client-ethernet-address](#)
- [no use-client-ethernet-address](#)
- [use-unicast-and-link-layer](#)
- [no use-unicast-and-link-layer](#)
- [diag advanced voip](#)
- [max-endpoints](#)
- [no max-endpoints](#)
- [odd-media-control-port](#)
- [no odd-media-control-port](#)
- [relax-quence-number-check](#)
- [no relax-quence-number-check](#)
- [auto-add-sip](#)
- [no auto-add-sip](#)
- [sip-transforms](#)
- [no sip-transforms](#)
- [invite-flush](#)
- [no invite-flush](#)
- [invite-flush-unused](#)
- [no invite-flush-unused](#)
- [reset sip-database](#)
- [bypass-sip-transformation](#)
- [no bypass-sip-transformation](#)
- [enforce-access-rule-check](#)
- [no enforce-access-rule-check](#)
- [diag advanced vpn](#)
- [adjust-tcp-mss](#)
- [no adjust-tcp-mss](#)
- [interoperable-ike-dh-exchange](#)
- [no interoperable-ike-dh-exchange](#)
- [fragment-after-esp](#)
- [no fragment-after-esp](#)
- [spi-cpi-parameter-index](#)
- [no spi-cpi-parameter-index](#)
- [trust-built-in-ca](#)
- [no trust-built-in-ca](#)
- [preserve-ike-port](#)
- [no preserve-ike-port](#)
- [diag advanced encryption](#)
- [hardware-encryption](#)
- [no hardware-encryption](#)
- [ssl-v3](#)
- [no ssl-v3](#)
- [tls-v1](#)
- [no tls-v1](#)
- [diag advanced firewall](#)
- [kill-cache-no-delay](#)
- [no kill-cache-no-delay](#)
- [ftp-bounce-attack-protection](#)
- [no ftp-bounce-attack-protection](#)
- [ftp-protocol-anomaly-attack-protection](#)
- [no ftp-protocol-anomaly-attack-protection](#)
- [orphan-data-connection](#)
- [no orphan-data-connection](#)
- [allow-zero-Port](#)

- [no allow-zero-Port](#)
- [ip-spoof-checking](#)
- [no ip-spoof-checking](#)
- [port-scan-detection](#)
- [no port-scan-detection](#)
- [ucapl-compliance](#)
- [no ucapl-compliance](#)
- [anticipated-connection-timeout](#)
- [no anticipated-connection-timeout](#)
- [anticipated-connection-parent-termination](#)
- [no anticipated-connection-parent-termination](#)
- [cache-ignore-icmp-reject](#)
- [no cache-ignore-icmp-reject](#)
- [anticipated-media-timeout](#)
- [no anticipated-media-timeout](#)
- [anticipated-media-parent-termination](#)
- [no anticipated-media-parent-termination](#)
- [trace-connections-port](#)
- [no trace-connections-port](#)
- [include-tcp-data-connection](#)
- [no include-tcp-data-connection](#)
- [track-bandwidth-usage](#)
- [no track-bandwidth-usage](#)
- [decrease-connection-count-after-close](#)
- [no decrease-connection-count-after-close](#)
- [csrf-token-validation](#)
- [no csrf-token-validation](#)
- [secure-session-id-cookie](#)
- [no secure-session-id-cookie](#)
- [tcp-state-manipulation-dos-protection](#)
- [no tcp-state-manipulation-dos-protection](#)
- [sequential-addresses](#)
- [no sequential-addresses](#)
- [default-policy-editable](#)
- [no default-policy-editable](#)
- [udp-icmp-flood-detecting](#)
- [no udp-icmp-flood-detecting](#)
- [udp-icmp-flood-protection](#)
- [no udp-icmp-flood-protection](#)
- [bypass-vpn-traffic](#)
- [no bypass-vpn-traffic](#)
- [log-object-name](#)
- [no log-object-name](#)
- [clear connections](#)
- [reset-login-counter](#)
- [no reset-login-counter](#)
- [send-rst-on-timeout](#)
- [no send-rst-on-timeout](#)
- [async-save-flash-period](#)
- [diag advanced security-services](#)
- [dpi-engine](#)
- [no dpi-engine](#)
- [bidirectional-ips](#)
- [no bidirectional-ips](#)
- [dpi-ip-fragment-reassembly](#)
- [no dpi-ip-fragment-reassembly](#)
- [dev-debug](#)
- [no dev-debug](#)
- [tcp-sequence-adjustment](#)
- [no tcp-sequence-adjustment](#)
- [proxy-email-packets](#)
- [no proxy-email-packets](#)
- [smtp-chunking-modification](#)
- [no smtp-chunking-modification](#)
- [pop3-auto-deletion](#)
- [no pop3-auto-deletion](#)
- [pop3-uidl-rewriting](#)
- [no pop3-uidl-rewriting](#)
- [smb-read-write-enforcement](#)
- [no smb-read-write-enforcement](#)
- [keep-http-accept-range-bytes](#)
- [no keep-http-accept-range-bytes](#)
- [log-virus-uri](#)
- [no log-virus-uri](#)
- [offset-qualifier-signature](#)
- [no offset-qualifier-signature](#)
- [minimum-http-header-length](#)
- [no minimum-http-header-length](#)
- [incremental-signature-updates](#)
- [no incremental-signature-updates](#)
- [handle-http2](#)
- [no handle-http2](#)
- [force-utm-offload](#)
- [no force-utm-offload](#)
- [utm-traffic-offload](#)
- [no utm-traffic-offload](#)
- [limit-dpi-tcp-window-advertisement](#)
- [no limit-dpi-tcp-window-advertisement](#)
- [threshold-limit](#)
- [maximum-regex-automaton-size](#)
- [signature-database-reload](#)
- [no signature-database-reload](#)

- [process-ips-signatures](#)
- [no process-ips-signatures](#)
- [process-gav-signatures](#)
- [no process-gav-signatures](#)
- [process-anti-spyware-signatures](#)
- [no process-anti-spyware-signatures](#)
- [process-app-signatures](#)
- [no process-app-signatures](#)
- [optimal-value](#)
- [no optimal-value](#)
- [limit-ips-cft-scan](#)
- [no limit-ips-cft-scan](#)
- [enforce-cfs-host-tag-search](#)
- [no enforce-cfs-host-tag-search](#)
- [local-cfs-server](#)
- [no local-cfs-server](#)
- [reset licenses](#)
- [reset http-clientless-notification-cache](#)
- [reset cloud-av-cache](#)
- [cloud-av-server](#)
- [no cloud-av-server](#)
- [reset cfs-memory-cache](#)
- [reset cfs-persistent-cache](#)
- [reset client-enforcement-status-info](#)
- [reset registration-log](#)
- [diag advanced dpi-ssl](#)
- [rewritten-certificate-sn-modifier](#)
- [client-spoofed-certificate-caching](#)
- [no client-spoofed-certificate-caching](#)
- [remove-tcp-timestamp-option](#)
- [no remove-tcp-timestamp-option](#)
- [drop-ssl-on-low-memory](#)
- [no drop-ssl-on-low-memory](#)
- [proxyless-ssl-when-limit-exceeded](#)
- [no proxyless-ssl-when-limit-exceeded](#)
- [endpoint-tcp-window-setup](#)
- [no endpoint-tcp-window-setup](#)
- [server-facing-session-reuse](#)
- [no server-facing-session-reuse](#)
- [client-facing-session-reuse](#)
- [no client-facing-session-reuse](#)
- [ip-based-exclusion-cache](#)
- [no ip-based-exclusion-cache](#)
- [use-2048-bit-certificate-key](#)
- [no use-2048-bit-certificate-key](#)
- [dynamic-exclusion-for-excluded-connections](#)
- [no dynamic-exclusion-for-excluded-connections](#)
- [connection-failures max-supported-entries](#)
- [connection-failures max-similar-failures](#)
- [connection-failures rollover-failed-entries](#)
- [no connection-failures rollover-failed-entries](#)
- [revocation-check-server-certificate](#)
- [no revocation-check-server-certificate](#)
- [expired-certificate-authority](#)
- [no expired-certificate-authority](#)
- [block-untrusted-certificate-connections](#)
- [no block-untrusted-certificate-connections](#)
- [max-stream-offset](#)
- [no max-stream-offset](#)
- [tcp-window-multiplier](#)
- [tcp-min-adv-window](#)
- [tcp-duplicate-ack-response-threshold](#)
- [extended-memory-implementation](#)
- [max-proxied-connections](#)
- [no max-proxied-connections](#)
- [update-security-services-info](#)
- [clear internal-session-and-cache-state](#)
- [ssl-version](#)
- [cipher-method](#)
- [diag advanced high-availability](#)
- [idle-monitor](#)
- [no idle-monitor](#)
- [suppress-active-transition-alarm](#)
- [no suppress-active-transition-alarm](#)
- [multi-chassis-lag](#)
- [no multi-chassis-lag](#)
- [restart-backup-on-watchdog](#)
- [no restart-backup-on-watchdog](#)
- [interleave-cache](#)
- [no interleave-cache](#)
- [transparent-mode-gratuitous-arp](#)
- [no transparent-mode-gratuitous-arp](#)
- [max-transparent-mode-gratuitous-arps](#)
- [max-gratuitous-arps](#)
- [diag advanced pppoe](#)
- [lcp-requests](#)
- [no lcp-requests](#)
- [log-lcp-echo](#)
- [no log-lcp-echo](#)
- [end-of-list-tag](#)
- [no end-of-list-tag](#)
- [netmask](#)

- [no netmask](#)
- [diag advanced dial-up](#)
- [max-pppdu-failure](#)
- [reset](#)
- [diag advanced dpi-stateful-firewall-security](#)
- [diag advanced stateful-firewall-security](#)
- [diag advanced management](#)
- [sonicui7-as-default](#)
- [no sonicui7-as-default](#)
- [new-license-page-format](#)
- [no new-license-page-format](#)
- [standby-management-sa](#)
- [no standby-management-sa](#)
- [gms-preempts-admin](#)
- [no gms-preempts-admin](#)
- [http-management](#)
- [no http-management](#)
- [classic-view](#)
- [no classic-view](#)
- [online-help-url](#)
- [diag advanced user-authentication](#)
- [post-authentication-redirect-url](#)
- [no post-authentication-redirect-url](#)
- [redirect-https](#)
- [no redirect-https](#)
- [https-redirect-port](#)
- [flush-cached-redirect-files](#)
- [logout users](#)
- [kill inactive-users](#)
- [log-all-sso-attempts](#)
- [no log-all-sso-attempts](#)
- [user-ip](#)
- [include-sso-polling](#)
- [no include-sso-polling](#)
- [include-sso-bypass](#)
- [no include-sso-bypass](#)
- [include-additional-non-initiation](#)
- [no include-additional-non-initiation](#)
- [sso-agent-version-negotiation](#)
- [no sso-agent-version-negotiation](#)
- [diag advanced diagnostics](#)
- [setup-tool-server](#)
- [no setup-tool-server](#)
- [trace-message-level](#)
- [auto-restart](#)
- [no auto-restart](#)
- [secured-crash-analysis](#)
- [no secured-crash-analysis](#)
- [show-user-diagnostics](#)
- [no show-user-diagnostics](#)
- [wan-connectivity-test start](#)
- [wan-connectivity-test target-ip](#)
- [no wan-connectivity-test target-ip](#)
- [wan-connectivity-test stop](#)
- [send wan-connectivity-test log](#)
- [dp-jobs-tracked](#)
- [suspend-assert-failure-task](#)
- [no suspend-assert-failure-task](#)
- [check-potential-deadlocks](#)
- [no check-potential-deadlocks](#)
- [diag advanced watchdog](#)
- [cpu-watchdog](#)
- [no cpu-watchdog](#)
- [restart-for](#)
- [no restart-for](#)
- [quick-restart](#)
- [no quick-restart](#)
- [restart-when-no-packet-rx](#)
- [no restart-when-no-packet-rx](#)
- [wait-for-no-packet-rx](#)
- [diag advanced wireless](#)
- [regulatory-domain](#)
- [no regulatory-domain](#)
- [sonicpoint support-type](#)
- [sonicpoint self-maintenance](#)
- [no sonicpoint self-maintenance](#)
- [vap-bssid-local-bit](#)
- [no vap-bssid-local-bit](#)
- [sonicpoint legacy-management](#)
- [no sonicpoint legacy-management](#)
- [sonicpoint update-firmware](#)
- [sonicpoint keepalive-enforcement](#)
- [no sonicpoint keepalive-enforcement](#)
- [sonicpoint profile-tcp-window-size](#)
- [no sonicpoint profile-tcp-window-size](#)
- [sonicpoint default-window-size](#)
- [no sonicpoint default-window-size](#)
- [sonicpointn ssh-management](#)
- [no sonicpointn ssh-management](#)
- [sonicpointn logging](#)
- [no sonicpointn logging](#)
- [sonicpoint erase-old-crash-log](#)

- [no sonicpoint erase-old-crash-log](#)
- [sonicpointn noise-security-level](#)
- [no sonicpointn noise-security-level](#)
- [sonicpointn noise-safemode-reboot](#)
- [no sonicpointn noise-safemode-reboot](#)
- [sonicpoint retain-ip](#)
- [no sonicpoint retain-ip](#)
- [sonicpoint snap-header](#)
- [no sonicpoint snap-header](#)
- [sonicpoint fragment-icmp](#)
- [no sonicpoint fragment-icmp](#)
- [bonjour-intra-wlan](#)
- [no bonjour-intra-wlan](#)
- [dhcp-arp-enhancement](#)
- [no dhcp-arp-enhancement](#)
- [guest-services-redirect-interval](#)
- [wifisec-enforcement](#)
- [no wifisec-enforcement](#)
- [wlan reply-wifisec-enforcement](#)
- [no wlan reply-wifisec-enforcement](#)
- [wlan dp-core-processing](#)
- [no wlan dp-core-processing](#)
- [wlan broadcast-communication](#)
- [no wlan broadcast-communication](#)
- [wlan bypass-gateway-firewalling](#)
- [no wlan bypass-gateway-firewalling](#)
- [wlan inter-client-communication](#)
- [no wlan inter-client-communication](#)
- [wlan ignore-check-ess](#)
- [no wlan ignore-check-ess](#)
- [wlan legacy-intel-client](#)
- [no wlan legacy-intel-client](#)
- [wlan nosiy-enviroment-enhancement](#)
- [no wlan nosiy-enviroment-enhancement](#)
- [wlan internal-dhcp](#)
- [no wlan internal-dhcp](#)
- [diag advanced tooltip-no-description](#)
- [no diag advanced tooltip-no-description](#)
- [diag advanced preference](#)
- [launching-conversion-control](#)
- [no launching-conversion-control](#)
- [processor-server](#)
- [no processor-server](#)
- [secure-http-to-processor](#)
- [no secure-http-to-processor](#)
- [site-relative-directory](#)
- [no site-relative-directory](#)
- [check-when-importing](#)
- [no check-when-importing](#)
- [diag advanced anti-spam](#)
- [syn-flood-protection](#)
- [no syn-flood-protection](#)
- [check-grid-ip-only](#)
- [no check-grid-ip-only](#)
- [outbound-smtp-grid-ip](#)
- [no outbound-smtp-grid-ip](#)
- [disabling-custom-email](#)
- [no disabling-custom-email](#)
- [limited-admin-configuration](#)
- [no limited-admin-configuration](#)
- [shlo-check](#)
- [no shlo-check](#)
- [auto-generated-cass-acl](#)
- [no auto-generated-cass-acl](#)
- [clear statistics](#)
- [reset grid-name-cache](#)
- [no policies-and-objects](#)
- [cass cloud service addr](#)
- [diag advanced hosted-email-security](#)
- [no diag advanced hosted-email-security](#)
- [diag advanced email-detection](#)
- [no diag advanced email-detection](#)
- [diag advanced remote-assistance](#)
- [no diag advanced remote-assistance](#)
- [diag advanced sslvpn](#)
- [netextender-version](#)
- [no netextender-version](#)
- [diag advanced backend-server](#)
- [enable](#)
- [no enable](#)
- [force-through](#)
- [diag advanced wan-acceleration](#)
- [remote-checking](#)
- [no remote-checking](#)
- [bypass-tcp-acceleration](#)
- [no bypass-tcp-acceleration](#)
- [skip-tcp-acceleration](#)
- [no skip-tcp-acceleration](#)
- [clear debug-status](#)
- [clear tcp-acceleration-database](#)
- [diag advanced geoip-location-service](#)
- [remote-geoip-server](#)

- [clear location-cache](#)
- [use-control-plane](#)
- [no use-control-plane](#)
- [bypass-geoip-blocking](#)
- [no bypass-geoip-blocking](#)
- [bypass-botnet-blocking](#)
- [no bypass-botnet-blocking](#)
- [geoip-botnet-map-file-upload](#)
- [no geoip-botnet-map-file-upload](#)
- [diag advanced flow-reporting](#)
- [clear location-map](#)
- [export-raw-database](#)
- [no export-raw-database](#)
- [sql-console](#)
- [no sql-console](#)
- [appflow-monitor-browser-frame-launch](#)
- [no appflow-monitor-browser-frame-launch](#)
- [non-admin-visualization](#)
- [no non-admin-visualization](#)
- [database-busy-timeout](#)
- [no database-busy-timeout](#)
- [hide-appflow-server](#)
- [no hide-appflow-server](#)
- [hide-gmsflow-server](#)
- [no hide-gmsflow-server](#)
- [report-server-address](#)
- [https-upload](#)
- [no https-upload](#)
- [clear database-tables](#)
- [diag advanced log-reschedule](#)
- [no diag advanced log-reschedule](#)
- [diag advanced ipv6 ready-enforce](#)
- [no diag advanced ipv6 ready-enforce](#)
- [diag advanced ipv6 allow-ndp-packet-less-than-255](#)
- [no diag advanced ipv6 allow-ndp-packet-less-than-255](#)
- [diag advanced ipv6 ndp-proxy-nat-ranges](#)
- [no diag advanced ipv6 ndp-proxy-nat-ranges](#)
- [diag advanced icmp drop-unreachable-packet](#)
- [no diag advanced icmp drop-unreachable-packet](#)
- [diag advanced icmp drop-exceeded-packet](#)
- [no diag advanced icmp drop-exceeded-packet](#)
- [diag advanced debug suppress-task-lock](#)
- [no diag advanced debug suppress-task-lock](#)
- [diag advanced debug suppress-task-dead-warning](#)
- [no diag advanced debug suppress-task-dead-warning](#)
- [diag advanced debug suppress-performance-testing-warning](#)
- [no diag advanced debug suppress-performance-testing-warning](#)
- [diag advanced network-fo-lb](#)
- [pers-idle-expire-time](#)
- [no pers-idle-expire-time](#)
- [pers-activity-interval](#)
- [pers-reuse-max](#)
- [no pers-reuse-max](#)
- [pers-src-ipaddr](#)
- [no pers-src-ipaddr](#)
- [pers-dst-ipaddr](#)
- [no pers-dst-ipaddr](#)
- [diag advanced trace-log](#)
- [cpu-util-check](#)
- [no cpu-util-check](#)
- [cpu-util-threshold](#)
- [no cpu-util-threshold](#)
- [clear trace-log](#)
- [diag advanced fqdn-dyn-addr-obj](#)
- [cache-dns-reply](#)
- [no cache-dns-reply](#)
- [offset-for-fqdn-objects](#)
- [no offset-for-fqdn-objects](#)
- [refresh-sub-domains](#)
- [no refresh-sub-domains](#)
- [donot-delete-expired-hosts](#)
- [no donot-delete-expired-hosts](#)
- [retain-expired-fqdn-hosts](#)
- [no retain-expired-fqdn-hosts](#)
- [unlimited-queries](#)
- [no unlimited-queries](#)
- [stop-dns-queries](#)
- [no stop-dns-queries](#)
- [max-retry-threshold](#)
- [min-allowed-til](#)
- [diag advanced cta-report](#)
- [use-secure-http](#)
- [no use-secure-http](#)
- [service-address type](#)
- [service-address ip](#)
- [no service-address ip](#)
- [service-http-port](#)
- [no service-http-port](#)
- [service-https-port](#)
- [no service-https-port](#)
- [upload-to-cloud-service](#)
- [no upload-to-cloud-service](#)

- [upload-to-yaml-format](#)
- [no upload-to-yaml-format](#)
- [support-for-ctav1-only](#)
- [no support-for-ctav1-only](#)
- [csc-reporting-cloud-fqdn](#)
- [no csc-reporting-cloud-fqdn](#)
- [diag advanced zero-touch](#)
- [restart](#)
- [enable](#)
- [disable](#)
- [fqdn-server](#)
- [server-ip-use-mode](#)
- [server-ip](#)
- [no server-ip](#)
- [reconnecting-delay](#)
- [no reconnecting-delay](#)
- [reconnecting-attempt](#)
- [no reconnecting-attempt](#)
- [skip-certificate](#)
- [no skip-certificate](#)
- [show-diagnostic-page](#)
- [no show-diagnostic-page](#)
- [debug-level](#)
- [no debug-level](#)
- [memory-free-call-tracking](#)
- [no memory-free-call-tracking](#)
- [ecli/packet-monitor.cdl](#)
 - [packet-monitor](#)
 - [start capture](#)
 - [stop capture](#)
 - [start mirror](#)
 - [stop mirror](#)
 - [log-to-ftp](#)
 - [export capture](#)
 - [monitor all](#)
 - [monitor default](#)
 - [clear capture](#)
 - [bytes-to-capture](#)
 - [wrap-buffer](#)
 - [no wrap-buffer](#)
 - [exclude encrypted-gms](#)
 - [no exclude encrypted-gms](#)
 - [exclude management](#)
 - [no exclude management](#)
 - [exclude syslog](#)
 - [no exclude syslog](#)
 - [exclude internal-traffic](#)
 - [no exclude internal-traffic](#)
 - [monitor-filter based-on-firewall-rule](#)
 - [no monitor-filter based-on-firewall-rule](#)
 - [monitor-filter interfaces](#)
 - [no monitor-filter interfaces](#)
 - [monitor-filter ether-types](#)
 - [no monitor-filter ether-types](#)
 - [monitor-filter ip-types](#)
 - [no monitor-filter ip-types](#)
 - [monitor-filter source-ips](#)
 - [no monitor-filter source-ips](#)
 - [monitor-filter source-ports](#)
 - [no monitor-filter source-ports](#)
 - [monitor-filter destination-ips](#)
 - [no monitor-filter destination-ips](#)
 - [monitor-filter destination-ports](#)
 - [no monitor-filter destination-ports](#)
 - [monitor-filter bidirectional](#)
 - [no monitor-filter bidirectional](#)
 - [monitor-filter status](#)
 - [no monitor-filter status](#)
 - [display-filter interfaces](#)
 - [no display-filter interfaces](#)
 - [display-filter ether-types](#)
 - [no display-filter ether-types](#)
 - [display-filter ip-types](#)
 - [no display-filter ip-types](#)
 - [display-filter source-ips](#)
 - [no display-filter source-ips](#)
 - [display-filter source-ports](#)
 - [no display-filter source-ports](#)
 - [display-filter destination-ips](#)
 - [no display-filter destination-ips](#)
 - [display-filter destination-ports](#)
 - [no display-filter destination-ports](#)
 - [display-filter bidirectional](#)
 - [no display-filter bidirectional](#)
 - [display-filter status](#)
 - [no display-filter status](#)
 - [ftp server](#)
 - [no ftp server](#)
 - [ftp login](#)
 - [no ftp login](#)
 - [ftp password](#)

- [no ftp password](#)
- [ftp directory](#)
- [no ftp directory](#)
- [ftp automatic](#)
- [no ftp automatic](#)
- [ftp pcapng](#)
- [no ftp pcapng](#)
- [ftp html](#)
- [no ftp html](#)
- [monitor-filter firewall-generated](#)
- [no monitor-filter firewall-generated](#)
- [monitor-filter intermediate](#)
- [no monitor-filter intermediate](#)
- [mirror max-rate](#)
- [mirror only-ip-packets](#)
- [no mirror only-ip-packets](#)
- [mirror interface](#)
- [no mirror interface](#)
- [mirror ip](#)
- [no mirror ip](#)
- [mirror receive-from-ip](#)
- [no mirror receive-from-ip](#)
- [mirror forward-interface](#)
- [no mirror forward-interface](#)
- [mirror to-capture-buffer](#)
- [no mirror to-capture-buffer](#)
- [mirror encrypt-key](#)
- [mirror decrypt-key](#)
- [ecli/tsr.cdl](#)
 - [send tech-support-report](#)
 - [tech-support-report options](#)
 - [sensitive-keys](#)
 - [no sensitive-keys](#)
 - [arp-cache](#)
 - [no arp-cache](#)
 - [dhcp-bindings](#)
 - [no dhcp-bindings](#)
 - [ike-info](#)
 - [no ike-info](#)
 - [wireless diagnostics](#)
 - [no wireless diagnostics](#)
 - [users](#)
 - [no users](#)
 - [ip-stack-info](#)
 - [no ip-stack-info](#)
 - [dns-proxy-cache](#)
 - [no dns-proxy-cache](#)
 - [debug-info](#)
 - [no debug-info](#)
 - [user-name](#)
 - [no user-name](#)
 - [ipv6 ndp](#)
 - [no ipv6 ndp](#)
 - [ipv6 dhcp](#)
 - [no ipv6 dhcp](#)
 - [geo-ip-cache](#)
 - [no geo-ip-cache](#)
 - [extra-routing](#)
 - [no extra-routing](#)
 - [atp-cache](#)
 - [no atp-cache](#)
 - [vendor-oui](#)
 - [no vendor-oui](#)
 - [ip-report](#)
 - [no ip-report](#)
 - [application-signature](#)
 - [no application-signature](#)
 - [abr-entries](#)
 - [no abr-entries](#)
 - [secured-crash-analysis](#)
 - [no secured-crash-analysis](#)
 - [secure-backup](#)
 - [no secure-backup](#)
 - [csc-report-time-interval](#)
 - [no csc-report-time-interval](#)
 - [send-raw-flow-data](#)
 - [no send-raw-flow-data](#)
- [ecli/packet-replay.cdl](#)
 - [no packet-replay-file](#)
 - [packet-replay](#)
 - [replay action-val](#)
 - [individual-replay action-val](#)
 - [replay-mac action-val](#)
 - [clear packets](#)
 - [refresh packets](#)
 - [packet-crafting-udp action-val](#)
 - [packet-crafting-icmp action-val](#)
 - [packet-crafting-jmp action-val](#)
 - [packet-crafting-buffer action-val](#)

- ecli/diag-ipnet.cdl
 - [diag_show ipnet](#)
- ecli/diag-advanced_show.cdl
 - [diag_show advanced](#)
- ecli/packet-monitor_show.cdl
 - [show packet-monitor](#)
- ecli/tsr_show.cdl
 - [show tech-support-report](#)
- ecli/debug_auth.cdl
 - [auth](#)
 - [tsa](#)
 - [cia](#)
 - [rad-acct](#)
 - [sso-api](#)
 - [radius](#)
 - [no radius](#)
 - [ldap](#)
 - [no ldap](#)
 - [tacacs](#)
 - [no tacacs](#)
- ecli/debug_user.cdl
 - [user](#)
 - [auth-level](#)
 - [ha-level](#)
 - [conn-level](#)
 - [ip-level](#)
- ecli/debug_ha.cdl
 - [ha](#)
 - [haf](#)
 - [no haf](#)
 - [haf-src](#)
 - [haf-dst](#)
 - [module](#)
 - [no module](#)
- ecli/debug_vpn.cdl
 - [vpn](#)
 - [cfg](#)
 - [gen](#)
 - [addnewln](#)
 - [no addnewln](#)
 - [matchlevel](#)
 - [no matchlevel](#)
 - [vpn](#)
 - [no vpn](#)
 - [ipsec](#)
 - [no ipsec](#)
 - [ike](#)
 - [no ike](#)
 - [module](#)
 - [no module](#)
- ecli/debug-cmd_show.cdl
 - [show dbg](#)
- ecli/address-object.cdl
 - [address-object ipv4](#)
 - [no address-object ipv4](#)
 - [address-object ipv6](#)
 - [no address-object ipv6](#)
 - [address-object mac](#)
 - [no address-object mac](#)
 - [address-object fqdn](#)
 - [no address-object fqdn](#)
 - [no address-objects](#)
 - [address-object resolve](#)
 - [address-object purge](#)
 - [address-group ipv4](#)
 - [no address-group ipv4](#)
 - [address-group ipv6](#)
 - [no address-group ipv6](#)
 - [no address-groups](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [host](#)
 - [no host](#)
 - [range](#)
 - [no range](#)
 - [network](#)
 - [no network](#)
 - [zone](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [address](#)
 - [no address](#)

- [zone](#)
- [multi-homed](#)
- [no multi-homed](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [domain](#)
- [no domain](#)
- [zone](#)
- [dns-ttl](#)
- [no dns-ttl](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [host](#)
- [no host](#)
- [range](#)
- [no range](#)
- [network](#)
- [no network](#)
- [zone](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [no address-object ipv4](#)
- [address-object ipv4](#)
- [no address-object mac](#)
- [address-object mac](#)
- [no address-object fqdn](#)
- [address-object fqdn](#)
- [no address-group ipv4](#)
- [address-group ipv4](#)
- [no address-group-members](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [no address-object ipv6](#)
- [address-object ipv6](#)
- [no address-group ipv6](#)
- [address-group ipv6](#)
- [ecli/schedule-object.cdl](#)
 - [scheduler](#)
 - [schedule](#)
 - [no schedule](#)
 - [no schedules](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [occurs](#)
 - [event](#)
 - [recurring](#)
 - [no recurring](#)
 - [no recurrings](#)
- [ecli/service-object.cdl](#)
 - [no service-object](#)
 - [no service-objects](#)
 - [service-object](#)
 - [no service-group](#)
 - [no service-groups](#)
 - [service-group](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [custom](#)
 - [icmp](#)
 - [igmp](#)
 - [tcp](#)
 - [udp](#)
 - [6over4](#)
 - [gre](#)
 - [esp](#)
 - [ah](#)
 - [icmpv6](#)
 - [icmpv6-custom](#)
 - [eigrp](#)
 - [ospf](#)
 - [pim](#)
 - [l2tp](#)
 - [ipcomp](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [no service-object](#)
 - [service-object](#)
 - [no service-group](#)
 - [service-group](#)
 - [no service-objects](#)
 - [no service-groups](#)
- [ecli/zone-object.cdl](#)

- [zone](#)
- [no zone](#)
- [no zones](#)
- [guest-services](#)
- [wireless](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [security-type](#)
- [no security-type](#)
- [interface-trust](#)
- [no interface-trust](#)
- [auto-generate-access-rules](#)
- [no auto-generate-access-rules](#)
- [websense-content-filtering](#)
- [no websense-content-filtering](#)
- [gateway-anti-virus](#)
- [no gateway-anti-virus](#)
- [intrusion-prevention](#)
- [no intrusion-prevention](#)
- [app-control](#)
- [no app-control](#)
- [anti-spyware](#)
- [no anti-spyware](#)
- [create-group-vpn](#)
- [no create-group-vpn](#)
- [ssl-control](#)
- [no ssl-control](#)
- [dpi-ssl-client](#)
- [no dpi-ssl-client](#)
- [dpi-ssl-server](#)
- [no dpi-ssl-server](#)
- [sslvpn-access](#)
- [no sslvpn-access](#)
- [enable](#)
- [no enable](#)
- [inter-guest](#)
- [no inter-guest](#)
- [external-auth](#)
- [captive-portal-authentication](#)
- [policy-page-non-authentication](#)
- [enable](#)
- [no enable](#)
- [client-redirect](#)
- [web-server-1 protocol](#)
- [no web-server-1](#)
- [web-server-2 protocol](#)
- [no web-server-2](#)
- [web-server timeout](#)
- [message-auth](#)
- [no message-auth](#)
- [social-network](#)
- [no social-network](#)
- [auth-pages web-server-1 login](#)
- [no auth-pages web-server-1 login](#)
- [auth-pages web-server-1 expiration](#)
- [no auth-pages web-server-1 expiration](#)
- [auth-pages web-server-1 timeout](#)
- [no auth-pages web-server-1 timeout](#)
- [auth-pages web-server-1 max-sessions](#)
- [no auth-pages web-server-1 max-sessions](#)
- [auth-pages web-server-1 traffic-exceeded](#)
- [no auth-pages web-server-1 traffic-exceeded](#)
- [auth-pages web-server-2 login](#)
- [no auth-pages web-server-2 login](#)
- [auth-pages web-server-2 expiration](#)
- [no auth-pages web-server-2 expiration](#)
- [auth-pages web-server-2 timeout](#)
- [no auth-pages web-server-2 timeout](#)
- [auth-pages web-server-2 max-sessions](#)
- [no auth-pages web-server-2 max-sessions](#)
- [auth-pages web-server-2 traffic-exceeded](#)
- [no auth-pages web-server-2 traffic-exceeded](#)
- [web-content redirect](#)
- [no web-content redirect](#)
- [web-content server-down](#)
- [no web-content server-down](#)
- [logout-expired](#)
- [no logout-expired](#)
- [status-check](#)
- [no status-check](#)
- [session-sync](#)
- [no session-sync](#)
- [enable](#)
- [no enable](#)
- [internal-url](#)
- [no internal-url](#)
- [external-url](#)
- [no external-url](#)
- [welcome-url-source](#)
- [no welcome-url-source](#)
- [welcome-url](#)

- [no welcome-url](#)
- [session-timeout-source](#)
- [no session-timeout-source](#)
- [session-timeout](#)
- [no session-timeout](#)
- [idle-timeout-source](#)
- [no idle-timeout-source](#)
- [idle-timeout](#)
- [no idle-timeout](#)
- [method](#)
- [no method](#)
- [enable](#)
- [no enable](#)
- [guest-usage-policy](#)
- [no guest-usage-policy](#)
- [idle-timeout](#)
- [no idle-timeout](#)
- [auto-accept](#)
- [no auto-accept](#)
- [custom-auth-page](#)
- [post-auth](#)
- [no post-auth](#)
- [bypass-guest-auth](#)
- [no bypass-guest-auth](#)
- [smtp-redirect](#)
- [no smtp-redirect](#)
- [deny-networks](#)
- [no deny-networks](#)
- [pass-networks](#)
- [no pass-networks](#)
- [max-guests](#)
- [enable](#)
- [no enable](#)
- [footer](#)
- [no footer](#)
- [header](#)
- [no header](#)
- [sslvpn-enforcement](#)
- [no sslvpn-enforcement](#)
- [wifi-sec-enforcement](#)
- [no wifi-sec-enforcement](#)
- [wifi-sec-for-site-to-site-vpn](#)
- [no wifi-sec-for-site-to-site-vpn](#)
- [trust-wpa-traffic-as-wifi-sec](#)
- [no trust-wpa-traffic-as-wifi-sec](#)
- [sonicpoint profile](#)
- [no sonicpoint profile](#)
- [bypass-gateway-firewalling](#)
- [no bypass-gateway-firewalling](#)
- [only-sonicpoint-traffic](#)
- [no only-sonicpoint-traffic](#)
- [auto-channel-limitation](#)
- [no auto-channel-limitation](#)
- [sonicwave-online-registration](#)
- [no sonicwave-online-registration](#)
- [sonicpoint-management](#)
- [no sonicpoint-management](#)
- [local-radius-server](#)
- [enable](#)
- [no enable](#)
- [interface-server-numbers](#)
- [port](#)
- [client-password](#)
- [no client-password](#)
- [tls-cache](#)
- [no tls-cache](#)
- [tls-cache-lifetime](#)
- [ldap-server](#)
- [enable](#)
- [no enable](#)
- [server](#)
- [no server](#)
- [base-dn](#)
- [no base-dn](#)
- [identity-dn](#)
- [no identity-dn](#)
- [identity-dn-password](#)
- [no identity-dn-password](#)
- [tls](#)
- [no tls](#)
- [cache](#)
- [no cache](#)
- [cache-lifetime](#)
- [active-directory-server](#)
- [enable](#)
- [no enable](#)
- [domain](#)
- [no domain](#)
- [full-name](#)
- [no full-name](#)
- [admin-user-name](#)
- [no admin-user-name](#)

- [admin-user-password](#)
- [no admin-user-password](#)
- [ecli/packet-dissection-object.cdl](#)
 - [no packet-dissection-object](#)
 - [no packet-dissection-objects](#)
 - [packet-dissection-object](#)
 - [no packet-dissection-group](#)
 - [no packet-dissection-groups](#)
 - [packet-dissection-group](#)
 - [name](#)
 - [negative-matching](#)
 - [no negative-matching](#)
 - [match-type](#)
 - [no packet-dissection-object](#)
 - [no packet-dissection-objects](#)
 - [packet-dissection-object](#)
 - [no packet-dissection-group](#)
 - [no packet-dissection-groups](#)
 - [packet-dissection-group](#)
 - [name](#)
 - [negative-matching](#)
 - [no negative-matching](#)
 - [family ipv4](#)
 - [family ipv6](#)
 - [family icmpv4](#)
 - [family icmpv6](#)
 - [family tcp](#)
 - [family udp](#)
 - [reserved](#)
 - [no reserved](#)
 - [dont-fragment](#)
 - [no dont-fragment](#)
 - [more-fragments](#)
 - [no more-fragments](#)
 - [fin](#)
 - [no fin](#)
 - [syn](#)
 - [no syn](#)
 - [rst](#)
 - [no rst](#)
 - [push](#)
 - [no push](#)
 - [ack](#)
 - [no ack](#)
 - [urg](#)
 - [no urg](#)
 - [ece](#)
 - [no ece](#)
 - [cwr](#)
 - [no cwr](#)
 - [data-type](#)
- [ecli/address-object_show.cdl](#)
 - [show address-objects](#)
 - [show address-object ipv4](#)
 - [show address-object ipv6](#)
 - [show address-object mac](#)
 - [show address-object fqdn](#)
 - [show address-groups](#)
 - [show address-group ipv4](#)
 - [show address-group ipv6](#)
- [ecli/schedule-object_show.cdl](#)
 - [show schedules](#)
 - [show schedule](#)
- [ecli/service-object_show.cdl](#)
 - [show service-objects](#)
 - [show service-object](#)
 - [show service-groups](#)
 - [show service-group](#)
- [ecli/zone-object_show.cdl](#)
 - [show zones](#)
 - [show zone](#)
- [ecli/packet-dissection-object_show.cdl](#)
 - [show packet-dissection-object](#)
 - [show packet-dissection-objects](#)
 - [show packet-dissection-group](#)
 - [show packet-dissection-groups](#)
- [ecli/interface.cdl](#)
 - [clear interface](#)
 - [interface-statistics display-all-traffic](#)
 - [no interface-statistics display-all-traffic](#)
 - [shutdown](#)
 - [no shutdown](#)
 - [interface](#)
 - [no interface](#)
 - [no interfaces vlan](#)
 - [no interfaces tunnel](#)

- [tunnel-interface 4to6](#)
- [no tunnel-interface 4to6](#)
- [no tunnel-interfaces 4to6](#)
- [name](#)
- [comment](#)
- [no comment](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [send-icmp-fragmentation](#)
- [no send-icmp-fragmentation](#)
- [fragment-packets](#)
- [no fragment-packets](#)
- [ignore-df-bit](#)
- [no ignore-df-bit](#)
- [type](#)
- [bound-to interface](#)
- [no bound-to](#)
- [bound-to interface](#)
- [no bound-to](#)
- [local](#)
- [remote](#)
- [local-ipv4](#)
- [no local-ipv4](#)
- [remote ipv6](#)
- [no remote](#)
- [local](#)
- [ip](#)
- [no ip](#)
- [tunnel-interface vpn](#)
- [no tunnel-interface vpn](#)
- [no tunnel-interfaces vpn](#)
- [policy](#)
- [renew](#)
- [release](#)
- [connect](#)
- [disconnect](#)
- [link-speed](#)
- [comment](#)
- [no comment](#)
- [bandwidth-management egress](#)
- [no bandwidth-management egress](#)
- [bandwidth-management ingress](#)
- [no bandwidth-management ingress](#)
- [send-icmp-fragmentation](#)
- [no send-icmp-fragmentation](#)
- [fragment-packets](#)
- [no fragment-packets](#)
- [ignore-df-bit](#)
- [no ignore-df-bit](#)
- [mtu](#)
- [https-redirect](#)
- [no https-redirect](#)
- [management](#)
- [no management](#)
- [user-login](#)
- [no user-login](#)
- [mac](#)
- [auto-discovery](#)
- [no auto-discovery](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [multicast](#)
- [no multicast](#)
- [cos-8021p](#)
- [no cos-8021p](#)
- [exclude-route](#)
- [no exclude-route](#)
- [asymmetric-route](#)
- [no asymmetric-route](#)
- [management-traffic-only](#)
- [no management-traffic-only](#)
- [dns-proxy](#)
- [no dns-proxy](#)
- [default-8021p-cos](#)
- [no default-8021p-cos](#)
- [shutdown-port](#)
- [no shutdown-port](#)
- [secondary ip](#)
- [no secondary ip](#)
- [secondary netmask](#)
- [no secondary netmask](#)
- [port aggregation aggregate](#)
- [no port aggregation aggregate](#)
- [port aggregation paired-aggregate](#)
- [no port aggregation paired-aggregate](#)
- [port redundancy](#)
- [no port redundancy-aggregation](#)
- [load-balancing-vip](#)
- [no load-balancing-vip](#)
- [routed-mode](#)
- [no routed-mode](#)
- [sonicpoint limit](#)

- [no sonicpoint limit](#)
- [sonicpoint reserve-address](#)
- [ip-assignment](#)
- [no ip-assignment](#)
- [native-bridge](#)
- [no native-bridge](#)
- [firewalling](#)
- [no firewalling](#)
- [type](#)
- [paired-interface](#)
- [no paired-interface](#)
- [paired-interface-zone](#)
- [stateful-inspection](#)
- [no stateful-inspection](#)
- [linkstate-propagation](#)
- [no linkstate-propagation](#)
- [restrict-analysis](#)
- [no restrict-analysis](#)
- [ip](#)
- [no ip](#)
- [netmask](#)
- [no netmask](#)
- [dns primary](#)
- [dns secondary](#)
- [dns tertiary](#)
- [no dns primary](#)
- [no dns secondary](#)
- [no dns tertiary](#)
- [one-arm-mode](#)
- [no one-arm-mode](#)
- [one-arm-peer](#)
- [no one-arm-peer](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [release](#)
- [renew](#)
- [renew-on-startup](#)
- [no renew-on-startup](#)
- [renew-on-link-up](#)
- [no renew-on-link-up](#)
- [initiate-renewals-with-discover](#)
- [no initiate-renewals-with-discover](#)
- [force-discover-interval](#)
- [no force-discover-interval](#)
- [schedule](#)
- [dynamic](#)
- [no dynamic](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [inactivity](#)
- [no inactivity](#)
- [ip](#)
- [no ip](#)
- [password](#)
- [no password](#)
- [release](#)
- [renew](#)
- [server](#)
- [no server](#)
- [user-name](#)
- [no user-name](#)
- [schedule](#)
- [dynamic](#)
- [no dynamic](#)
- [gateway](#)
- [no gateway](#)
- [hostname](#)
- [no hostname](#)
- [inactivity](#)
- [no inactivity](#)
- [ip](#)
- [no ip](#)
- [password](#)
- [no password](#)
- [release](#)
- [renew](#)
- [server](#)
- [no server](#)
- [shared-secret](#)
- [no shared-secret](#)
- [user-name](#)
- [no user-name](#)
- [dynamic](#)
- [no dynamic](#)
- [unnumbered](#)
- [no unnumbered](#)
- [inactivity](#)
- [no inactivity](#)

- [ip](#)
- [no ip](#)
- [lcp-echo-packets](#)
- [no lcp-echo-packets](#)
- [password](#)
- [no password](#)
- [service-name](#)
- [no service-name](#)
- [reconnect](#)
- [ncp_neg_retrans](#)
- [no reconnect](#)
- [user-name](#)
- [no user-name](#)
- [schedule](#)
- [bridge-to](#)
- [block-non-ip](#)
- [no block-non-ip](#)
- [route-on-bridge-pair](#)
- [no route-on-bridge-pair](#)
- [only-sniff](#)
- [no only-sniff](#)
- [stateful-inspection](#)
- [no stateful-inspection](#)
- [vlan-filtering-mode](#)
- [filtered-vlan](#)
- [no filtered-vlan](#)
- [no filtered-vlans](#)
- [no transparent-range](#)
- [transparent-range](#)
- [gratuitous-arp-wan-forwarding](#)
- [no gratuitous-arp-wan-forwarding](#)
- [gratuitous-arp-wan-generation](#)
- [no gratuitous-arp-wan-generation](#)
- [ecli/arp.cdl](#)
 - [arp](#)
 - [no entry](#)
 - [no entries](#)
 - [entry](#)
 - [timeout](#)
 - [glean](#)
 - [no glean](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [publish](#)
 - [no publish](#)
 - [bind-mac](#)
 - [no bind-mac](#)
 - [dynamic](#)
 - [no dynamic](#)
 - [clear arp cache entries](#)
 - [clear arp cache entry](#)
- [ecli/dns.cdl](#)
 - [dns server](#)
 - [no dns server](#)
 - [dns rebinding](#)
 - [no dns rebinding](#)
 - [dns fqdn-binding](#)
 - [no dns fqdn-binding](#)
 - [dns split-servers](#)
 - [no dns split-servers](#)
 - [no dns split-entries](#)
 - [no dns split-entry](#)
 - [dns split-entry](#)
 - [domain](#)
 - [no server ipv4](#)
 - [server ipv4](#)
 - [no server ipv6](#)
 - [server ipv6](#)
 - [no local-interface](#)
 - [local-interface](#)
 - [no manual-ttl](#)
 - [manual-ttl](#)
 - [dns fqdn-over-tcp-dns](#)
 - [no dns fqdn-over-tcp-dns](#)
 - [clear dns cache](#)
- [ecli/ddns.cdl](#)
 - [no dynamic-dns profile](#)
 - [no dynamic-dns profiles](#)
 - [dynamic-dns profile](#)
 - [profile-name](#)
 - [enable](#)
 - [no enable](#)
 - [use-online](#)
 - [no use-online](#)
 - [provider](#)
 - [user-name](#)
 - [no user-name](#)
 - [password](#)

- [no password](#)
- [domain](#)
- [no domain](#)
- [bound-to](#)
- [online-settings](#)
- [offline-settings](#)
- [service-type](#)
- [ecli/dhcp-server.cdl](#)
 - [dhcp-server](#)
 - [enable](#)
 - [no enable](#)
 - [conflict-detection](#)
 - [no conflict-detection](#)
 - [persistence](#)
 - [no persistence](#)
 - [persistence-monitoring-interval](#)
 - [scope dynamic](#)
 - [no scope dynamic](#)
 - [scope static](#)
 - [no scope static](#)
 - [no scopes dynamic](#)
 - [no scopes static](#)
 - [no scopes](#)
 - [clear lease](#)
 - [clear leases](#)
 - [option object](#)
 - [no option object](#)
 - [no option objects](#)
 - [option group](#)
 - [no option group](#)
 - [no option groups](#)
 - [trusted-relay-agents](#)
 - [no trusted-relay-agents](#)
 - [recycle-expired-lease](#)
 - [no recycle-expired-lease](#)
 - [enable](#)
 - [no enable](#)
 - [range](#)
 - [lease-time](#)
 - [default-gateway](#)
 - [no default-gateway](#)
 - [netmask](#)
 - [comment](#)
 - [no comment](#)
 - [allow-bootp](#)
 - [no allow-bootp](#)
 - [domain-name](#)
 - [no domain-name](#)
 - [dns server](#)
 - [no dns server](#)
 - [wins](#)
 - [no wins](#)
 - [call-manager](#)
 - [no call-manager](#)
 - [network-boot](#)
 - [no network-boot](#)
 - [no generic-option](#)
 - [generic-option](#)
 - [always-send-option](#)
 - [no always-send-option](#)
 - [enable](#)
 - [no enable](#)
 - [name](#)
 - [no name](#)
 - [ip](#)
 - [mac](#)
 - [lease-time](#)
 - [default-gateway](#)
 - [no default-gateway](#)
 - [netmask](#)
 - [comment](#)
 - [no comment](#)
 - [domain-name](#)
 - [no domain-name](#)
 - [dns server](#)
 - [no dns server](#)
 - [wins](#)
 - [no wins](#)
 - [call-manager](#)
 - [no call-manager](#)
 - [network-boot](#)
 - [no network-boot](#)
 - [no generic-option](#)
 - [generic-option](#)
 - [always-send-option](#)
 - [no always-send-option](#)
 - [name](#)
 - [number](#)
 - [array](#)
 - [no array](#)
 - [no value](#)

- [no values](#)
- [value](#)
- [name](#)
- [option object](#)
- [no option object](#)
- [option group](#)
- [no option group](#)
- [no members](#)
- [ecli/failover-load-balancing.cdl](#)
 - [clear failover-lb](#)
 - [failover-lb](#)
 - [enable](#)
 - [no enable](#)
 - [respond-to-probes](#)
 - [no respond-to-probes](#)
 - [any-tcp-syn](#)
 - [no any-tcp-syn](#)
 - [port](#)
 - [group](#)
 - [type](#)
 - [preempt](#)
 - [no preempt](#)
 - [spillover-bandwidth](#)
 - [no spillover-bandwidth](#)
 - [address-binding](#)
 - [no address-binding](#)
 - [auto-adjust-ratio](#)
 - [interface](#)
 - [no interface](#)
 - [no interfaces](#)
 - [final-backup](#)
 - [no final-backup](#)
 - [probing](#)
 - [health-check](#)
 - [missed-intervals](#)
 - [successful-intervals](#)
 - [global-responder](#)
 - [no global-responder](#)
 - [rank](#)
 - [percent](#)
 - [probe-type](#)
 - [probe-condition](#)
 - [main-target](#)
 - [no main-target](#)
 - [alternate-target](#)
 - [no alternate-target](#)
 - [default-target](#)
 - [no default-target](#)
- [ecli/ip-helper.cdl](#)
 - [ip-helper](#)
 - [enable](#)
 - [no enable](#)
 - [policy](#)
 - [no policy](#)
 - [no policies](#)
 - [protocol](#)
 - [no protocol](#)
 - [no protocols](#)
 - [enable](#)
 - [no enable](#)
 - [protocol](#)
 - [source](#)
 - [destination](#)
 - [comment](#)
 - [no comment](#)
 - [egressif](#)
 - [no egressif](#)
 - [name](#)
 - [enable](#)
 - [no enable](#)
 - [no port1](#)
 - [port1](#)
 - [no port2](#)
 - [port2](#)
 - [timeout](#)
 - [mode](#)
 - [multicast-ip](#)
 - [no multicast-ip](#)
 - [multicast-ipv6](#)
 - [source-translation](#)
 - [no source-translation](#)
 - [raw](#)
 - [no raw](#)
- [ecli/mac-ip-anti-spoof.cdl](#)
 - [mac-ip-anti-spoof](#)
 - [interface](#)
 - [interface](#)
 - [cache entry](#)
 - [no cache entry](#)

- [cache entry](#)
- [no cache entry](#)
- [no cache entries](#)
- [router](#)
- [no router](#)
- [blacklisted](#)
- [no blacklisted](#)
- [ip](#)
- [mac](#)
- [interface](#)
- [clear mac-ip-anti-spoof cache statistics ipv4](#)
- [clear mac-ip-anti-spoof spoof-detected-list ipv4](#)
- [resolve mac-ip-anti-spoof spoof-detected-list ipv4](#)
- [router](#)
- [no router](#)
- [blacklisted](#)
- [no blacklisted](#)
- [ip](#)
- [mac](#)
- [interface](#)
- [clear mac-ip-anti-spoof cache statistics ipv6](#)
- [clear mac-ip-anti-spoof spoof-detected-list ipv6](#)
- [resolve mac-ip-anti-spoof spoof-detected-list ipv6](#)
- [enable](#)
- [no enable](#)
- [static-arp](#)
- [no static-arp](#)
- [dhcp-server](#)
- [no dhcp-server](#)
- [dhcp-relay](#)
- [no dhcp-relay](#)
- [arp-lock](#)
- [no arp-lock](#)
- [arp-watch](#)
- [no arp-watch](#)
- [enforce-ingress](#)
- [no enforce-ingress](#)
- [spoof-detection](#)
- [no spoof-detection](#)
- [allow-management](#)
- [no allow-management](#)
- [enable](#)
- [no enable](#)
- [static-ndp](#)
- [no static-ndp](#)
- [ndp-lock](#)
- [no ndp-lock](#)
- [enforce-ingress](#)
- [no enforce-ingress](#)
- [spoof-detection](#)
- [no spoof-detection](#)
- [allow-management](#)
- [no allow-management](#)
- [ecli/nat.cdl](#)
 - [no nat-policy ipv4 inbound](#)
 - [no nat-policy ipv6 inbound](#)
 - [no nat-policy ipv4 uuid](#)
 - [no nat-policy ipv6 uuid](#)
 - [no nat-policies](#)
 - [nat-policy ipv4 inbound](#)
 - [nat-policy ipv6 inbound](#)
 - [nat-policy ipv4 uuid](#)
 - [nat-policy ipv6 uuid](#)
 - [no nat-policy nat64 inbound](#)
 - [no nat-policy nat64 uuid](#)
 - [nat-policy nat64 inbound](#)
 - [nat-policy nat64 uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [priority](#)
 - [comment](#)
 - [no comment](#)
 - [enable](#)
 - [no enable](#)
 - [dns-doctoring](#)
 - [no dns-doctoring](#)
 - [inbound](#)
 - [outbound](#)
 - [destination](#)
 - [source](#)
 - [service](#)
 - [reflexive](#)
 - [no reflexive](#)
 - [translated-destination](#)
 - [translated-source](#)

- [translated-service](#)
- [override-mac](#)
- [source](#)
- [translated-source](#)
- [pref64](#)
- [high-availability](#)
- [nat-method](#)
- [source-port-remap](#)
- [no source-port-remap](#)
- [probing](#)
- [no probing](#)
- [probe-every](#)
- [probe-type](#)
- [reply-timeout](#)
- [deactivate-after](#)
- [reactivate-after](#)
- [rst-as-miss](#)
- [no rst-as-miss](#)
- [port-probing](#)
- [no port-probing](#)
- [ticket tag1](#)
- [no ticket tag1](#)
- [ticket tag2](#)
- [no ticket tag2](#)
- [ticket tag3](#)
- [no ticket tag3](#)
- [clear nat-policy statistics](#)
- [ecli/network-monitor.cdl](#)
 - [no network-monitor policy](#)
 - [no network-monitor policies](#)
 - [clear network-monitor statistics](#)
 - [network-monitor policy](#)
 - [name](#)
 - [no probe target](#)
 - [probe target](#)
 - [next-hop](#)
 - [no next-hop](#)
 - [local-ip](#)
 - [no local-ip](#)
 - [outbound-interface](#)
 - [probe type](#)
 - [probe interval](#)
 - [reply-timeout](#)
 - [interval missed](#)
 - [interval successful](#)
 - [must-respond](#)
 - [no must-respond](#)
 - [rst-as-miss](#)
 - [no rst-as-miss](#)
 - [comment](#)
 - [no comment](#)
 - [uuid](#)
 - [no uuid](#)
- [ecli/routing.cdl](#)
 - [routing](#)
 - [mode](#)
 - [nsm](#)
 - [ospf](#)
 - [rip](#)
 - [ospfv3](#)
 - [ripng](#)
 - [no bgp](#)
 - [bgp](#)
 - [default-route-metric](#)
 - [metric-priority](#)
 - [no metric-priority](#)
 - [no route-policy ipv4 interface](#)
 - [no route-policy ipv6 interface](#)
 - [no route-policy ipv4 uuid](#)
 - [no route-policy ipv6 uuid](#)
 - [no route-policies](#)
 - [no route-policies-sdwan](#)
 - [no route-policies-ipv4](#)
 - [no route-policies-ipv6](#)
 - [route-policy ipv4 interface](#)
 - [route-policy ipv6 interface](#)
 - [route-policy ipv4 uuid](#)
 - [route-policy ipv6 uuid](#)
 - [no uuid](#)
 - [route-policy ipv6 uuid](#)
 - [no uuid](#)
 - [source](#)
 - [destination](#)
 - [service](#)
 - [app](#)
 - [application](#)
 - [gateway](#)
 - [tos](#)
 - [no tos](#)

- [mask](#)
- [no mask](#)
- [distance](#)
- [path-selection-profile](#)
- [no path-selection-profile](#)
- [interface](#)
- [gateway2](#)
- [interface2](#)
- [gateway3](#)
- [interface3](#)
- [gateway4](#)
- [interface4](#)
- [nexthop-number](#)
- [metric](#)
- [no name](#)
- [name](#)
- [no comment](#)
- [comment](#)
- [disable-on-interface-down](#)
- [no disable-on-interface-down](#)
- [vpn-precedence](#)
- [no vpn-precedence](#)
- [tcp-acceleration](#)
- [no tcp-acceleration](#)
- [wxa-group](#)
- [no wxa-group](#)
- [auto-add-access-rules](#)
- [no auto-add-access-rules](#)
- [probe](#)
- [no probe](#)
- [disable-when-probes-succeed](#)
- [no disable-when-probes-succeed](#)
- [default-probe-state-up](#)
- [no default-probe-state-up](#)
- [ticket tag1](#)
- [no ticket tag1](#)
- [ticket tag2](#)
- [no ticket tag2](#)
- [ticket tag3](#)
- [no ticket tag3](#)
- [ipv6 default-route-metric](#)
- [ecli/web-proxy.cdl](#)
 - [web-proxy](#)
 - [server](#)
 - [no server](#)
 - [port](#)
 - [no port](#)
 - [bypass-upon-failure](#)
 - [no bypass-upon-failure](#)
 - [forward-public-requests](#)
 - [no forward-public-requests](#)
 - [user-proxy-server](#)
 - [no user-proxy-server](#)
 - [no user-proxy-servers](#)
- [ecli/aws-configuration.cdl](#)
 - [amazon-web-services connection](#)
 - [access-key-id](#)
 - [no access-key-id](#)
 - [secret](#)
 - [no secret](#)
 - [region](#)
 - [connect](#)
 - [test](#)
- [ecli/aws-object.cdl](#)
 - [amazon-web-services objects](#)
 - [mapping](#)
 - [no mapping](#)
 - [synchronization-interval](#)
 - [monitor-region](#)
 - [no monitor-region](#)
 - [no address-objects](#)
 - [group-mapping](#)
 - [no group-mapping](#)
 - [no group-mappings](#)
 - [address-group](#)
 - [condition](#)
 - [no condition](#)
 - [no conditions](#)
- [ecli/neighbor-discovery.cdl](#)
 - [no ndp entry](#)
 - [no ndp entries](#)
 - [ndp reachable-time](#)
 - [no ndp reachable-time](#)
 - [ndp entry](#)
 - [ip](#)
 - [mac](#)
 - [interface](#)
 - [clear ndp cache entries](#)
 - [clear ndp cache entry](#)

- ecli/interface-ipv6.cdl
 - [tunnel-interface ipv6](#)
 - [no tunnel-interface ipv6](#)
 - [no tunnel-interfaces ipv6](#)
 - [name](#)
 - [zone](#)
 - [no zone](#)
 - [type](#)
 - [ip](#)
 - [no ip](#)
 - [prefix-length](#)
 - [comment](#)
 - [no comment](#)
 - [management](#)
 - [no management](#)
 - [user-login](#)
 - [no user-login](#)
 - [https-redirect](#)
 - [no https-redirect](#)
 - [remote ipv4-address](#)
 - [no remote ipv4-address](#)
 - [remote ipv6-network](#)
 - [no remote ipv6-network](#)
 - [bound-to](#)
 - [link-mtu](#)
 - [remote ipv4-address](#)
 - [no remote ipv4-address](#)
 - [remote ipv6-network](#)
 - [no remote ipv6-network](#)
 - [bound-to](#)
 - [link-mtu](#)
 - [bound-to](#)
 - [enable](#)
 - [no enable](#)
 - [link-mtu](#)
 - [bound-to](#)
 - [no bound-to](#)
 - [dynamic](#)
 - [no dynamic](#)
 - [6rd prefix](#)
 - [no 6rd prefix](#)
 - [6rd prefix-length](#)
 - [no 6rd prefix-length](#)
 - [border-relay-ipv4-address](#)
 - [no border-relay-ipv4-address](#)
 - [mask-length](#)
 - [no mask-length](#)
 - [link-mtu](#)
 - [default-route](#)
 - [no default-route](#)
 - [bound-to](#)
 - [no bound-to](#)
 - [prefix](#)
 - [no prefix](#)
 - [link-mtu](#)
 - [ipv6-traffic](#)
 - [no ipv6-traffic](#)
 - [listen-router-advertisement](#)
 - [no listen-router-advertisement](#)
 - [stateless-address-autoconfig](#)
 - [no stateless-address-autoconfig](#)
 - [duplicate-address-detection-transmits](#)
 - [no duplicate-address-detection-transmits](#)
 - [reachable-time](#)
 - [no reachable-time](#)
 - [ip-assignment](#)
 - [no ip-assignment](#)
 - [ip](#)
 - [no ip](#)
 - [prefix-length](#)
 - [dns primary](#)
 - [dns secondary](#)
 - [dns tertiary](#)
 - [no dns primary](#)
 - [no dns secondary](#)
 - [no dns tertiary](#)
 - [gateway](#)
 - [no gateway](#)
 - [advertise-subnet-prefix](#)
 - [no advertise-subnet-prefix](#)
 - [extra-ip](#)
 - [no extra-ip](#)
 - [no extra-ipv6-addresses](#)
 - [router-advertisement](#)
 - [one-arm-mode](#)
 - [no one-arm-mode](#)
 - [one-arm-peer](#)
 - [no one-arm-peer](#)
 - [multicast](#)
 - [no multicast](#)
 - [type](#)
 - [ip](#)

- [prefix-length](#)
- [delegated-prefix](#)
- [no delegated-prefix](#)
- [preferred-ip](#)
- [preferred-prefix-length](#)
- [no preferred-prefix-length](#)
- [advertise-subnet-prefix](#)
- [no advertise-subnet-prefix](#)
- [enable](#)
- [no enable](#)
- [interval](#)
- [link-mtu](#)
- [no link-mtu](#)
- [reachable-time](#)
- [no reachable-time](#)
- [retransmit-timer](#)
- [no retransmit-timer](#)
- [current-hop-limit](#)
- [no current-hop-limit](#)
- [router lifetime](#)
- [no router lifetime](#)
- [router preference](#)
- [managed](#)
- [no managed](#)
- [other-config](#)
- [no other-config](#)
- [prefix](#)
- [no prefix](#)
- [no prefixes](#)
- [prefix](#)
- [valid-lifetime](#)
- [no valid-lifetime](#)
- [preferred lifetime](#)
- [no preferred lifetime](#)
- [on-link](#)
- [no on-link](#)
- [autonomous](#)
- [no autonomous](#)
- [prefix-delegation](#)
- [no prefix-delegation](#)
- [rapid-commit](#)
- [no rapid-commit](#)
- [after-name-option](#)
- [no after-name-option](#)
- [release](#)
- [renew](#)
- [mode-assignment](#)
- [nbp-neg-retrans](#)
- [schedule](#)
- [inactivity](#)
- [no inactivity](#)
- [lcp-echo-packets](#)
- [no lcp-echo-packets](#)
- [reconnect](#)
- [no reconnect](#)
- [ecli/dhcp-server-ipv6.cdl](#)
 - [enable](#)
 - [no enable](#)
 - [option object](#)
 - [no option object](#)
 - [no option objects](#)
 - [name](#)
 - [number](#)
 - [array](#)
 - [no array](#)
 - [value](#)
 - [no value](#)
 - [option group](#)
 - [no option group](#)
 - [no option groups](#)
 - [name](#)
 - [option object](#)
 - [no option object](#)
 - [option group](#)
 - [no option group](#)
 - [scope dynamic](#)
 - [no scope dynamic](#)
 - [no scopes dynamic](#)
 - [name](#)
 - [enable](#)
 - [no enable](#)
 - [prefix](#)
 - [no prefix](#)
 - [range](#)
 - [no range](#)
 - [lifetime valid](#)
 - [no lifetime valid](#)
 - [lifetime preferred](#)
 - [no lifetime preferred](#)
 - [comment](#)
 - [no comment](#)

- [always-send-option](#)
- [no always-send-option](#)
- [domain-name](#)
- [no domain-name](#)
- [dns server](#)
- [no dns server](#)
- [generic-option](#)
- [no generic-option](#)
- [scope static](#)
- [no scope static](#)
- [no scopes static](#)
- [enable](#)
- [no enable](#)
- [name](#)
- [no name](#)
- [prefix](#)
- [no prefix](#)
- [ip](#)
- [no ip](#)
- [iaid](#)
- [no iaaid](#)
- [duid](#)
- [no duuid](#)
- [lifetime](#)
- [no lifetime](#)
- [comment](#)
- [no comment](#)
- [always-send-option](#)
- [no always-send-option](#)
- [domain-name](#)
- [no domain-name](#)
- [dns server](#)
- [no dns server](#)
- [generic-option](#)
- [no generic-option](#)
- [clear lease](#)
- [clear leases](#)
- [ecli/dns-proxy.cdl](#)
 - [dns-proxy](#)
 - [enable](#)
 - [no enable](#)
 - [mode](#)
 - [protocol](#)
 - [enforce-all-dns-requests](#)
 - [no enforce-all-dns-requests](#)
 - [dns-cache](#)
 - [no dns-cache](#)
 - [no cache-entries](#)
 - [no cache-entry](#)
 - [cache-entry](#)
 - [domain](#)
 - [no address ipv4](#)
 - [address ipv4](#)
 - [no address ipv6](#)
 - [address ipv6](#)
 - [flush cache-entry](#)
 - [flush cache-entries](#)
- [ecli/vlan-translation.cdl](#)
 - [vlan-translation](#)
 - [no vlan-translation](#)
 - [no vlan-translations](#)
 - [ingress interface](#)
 - [ingress vlan](#)
 - [egress interface](#)
 - [egress vlan](#)
 - [reverse](#)
 - [no reverse](#)
- [ecli/dns-security.cdl](#)
 - [dns-security](#)
 - [dns-sinkhole](#)
 - [enable](#)
 - [no enable](#)
 - [action-type](#)
 - [no custom-malicious-entries](#)
 - [no custom-malicious-entry](#)
 - [custom-malicious-entry](#)
 - [no white-list-entries](#)
 - [no white-list-entry](#)
 - [white-list-entry](#)
 - [dns-tunnel](#)
 - [enable](#)
 - [no enable](#)
 - [block-all](#)
 - [no block-all](#)
 - [no white-list-entries](#)
 - [no white-list-entry](#)
 - [white-list-entry](#)
 - [block](#)
 - [no block](#)

- ecli/portshield-groups.cdl
 - [portshield-groups](#)
 - [no external-switch](#)
 - [no external-switches](#)
 - [external-switch](#)
 - [id](#)
 - [switch-model](#)
 - [ip](#)
 - [user-name](#)
 - [password](#)
 - [switch-mode](#)
 - [parent-switch-id](#)
 - [parent-switch-uplink](#)
 - [no parent-switch-uplink](#)
 - [switch-management](#)
 - [secondary-switch-management](#)
 - [firewall-uplink](#)
 - [no firewall-uplink](#)
 - [switch-uplink](#)
 - [no switch-uplink](#)
 - [secondary-switch-uplink](#)
 - [no secondary-switch-uplink](#)
 - [stp-mode](#)
 - [stp-state](#)
 - [no stp-state](#)
 - [poe-alert-usage-threshold](#)
 - [poe-traps](#)
 - [no poe-traps](#)
 - [poe-power-limit-mode](#)
 - [poe-management-mode](#)
 - [poe-detection-type](#)
- ecli/interface_show.cdl
 - [show tunnel-interface 4to6](#)
 - [show tunnel-interfaces 4to6](#)
 - [show interfaces](#)
 - [show interface](#)
 - [show switch-statdump](#)
 - [show tunnel-interface vpn](#)
 - [show tunnel-interfaces vpn](#)
- ecli/arp_show.cdl
 - [show arp](#)
- ecli/dns_show.cdl
 - [show dns](#)
- ecli/ddns_show.cdl
 - [show dynamic-dns profiles](#)
 - [show dynamic-dns profile](#)
- ecli/dhcp-server_show.cdl
 - [show dhcp-server](#)
- ecli/failover-load-balancing_show.cdl
 - [show failover-lb](#)
- ecli/ip-helper_show.cdl
 - [show ip-helper](#)
- ecli/mac-ip-anti-spoof_show.cdl
 - [show mac-ip-anti-spoof](#)
- ecli/nat_show.cdl
 - [show nat-policies](#)
 - [show nat-policy ipv4 inbound](#)
 - [show nat-policy ipv6 inbound](#)
 - [show nat-policy nat64 inbound](#)
 - [show nat-policy ipv4 uuid](#)
 - [show nat-policy ipv6 uuid](#)
 - [show nat-policy nat64 uuid](#)
- ecli/network-monitor_show.cdl
 - [show network-monitor policies](#)
 - [show network-monitor policy](#)
- ecli/routing_show.cdl
 - [show routing mode](#)
 - [show route-policies](#)
 - [show route-policy ipv4 interface](#)
 - [show route-policy ipv6 interface](#)
 - [show route-policy ipv4 uuid](#)
 - [show route-policy ipv6 uuid](#)
 - [show routing nsm](#)
 - [show routing rip](#)
 - [show routing ospf](#)
 - [show routing bgp](#)
 - [show routing ripng](#)
 - [show routing ospfv3](#)
- ecli/web-proxy_show.cdl
 - [show web-proxy](#)
- ecli/aws-configuration_show.cdl

- [show amazon-web-services connection](#)
- ecli/aws-object_show.cdl
 - [show amazon-web-services objects](#)
- ecli/neighbor-discovery_show.cdl
 - [show ndp](#)
- ecli/interface-ipv6_show.cdl
 - [show tunnel-interface ipv6](#)
 - [show tunnel-interfaces ipv6](#)
- ecli/dns-proxy_show.cdl
 - [show dns-proxy](#)
- ecli/vlan-translation_show.cdl
 - [show vlan-translation](#)
 - [show vlan-translations](#)
- ecli/dns-security_show.cdl
 - [show dns-security](#)
- ecli/portshield-groups_show.cdl
 - [show portshield-groups](#)
 - [show portshield](#)
- ecli/firewall.cdl
 - [firewall](#)
 - [security-services-enforcement global](#)
 - [security-services-enforcement policy](#)
 - [stealth-mode](#)
 - [no stealth-mode](#)
 - [randomize-id](#)
 - [no randomize-id](#)
 - [decrement ttl](#)
 - [no decrement ttl](#)
 - [icmp time-exceeded-packets](#)
 - [no icmp time-exceeded-packets](#)
 - [ftp-transforms-in-service-object](#)
 - [sqlnet](#)
 - [no sqlnet](#)
 - [rtsp-transformations](#)
 - [no rtsp-transformations](#)
 - [drop source-routed](#)
 - [no drop source-routed](#)
 - [drop source-subnet-broadcast](#)
 - [no drop source-subnet-broadcast](#)
 - [starting-vlan](#)
 - [connections](#)
 - [force-ftp-data](#)
 - [no force-ftp-data](#)
 - [apply-rules-for-intra-lan](#)
 - [no apply-rules-for-intra-lan](#)
 - [issue-rst-for-outgoing-discards](#)
 - [no issue-rst-for-outgoing-discards](#)
 - [icmp redirect-on-lan](#)
 - [no icmp redirect-on-lan](#)
 - [ip checksum-enforcement](#)
 - [no ip checksum-enforcement](#)
 - [udp checksum-enforcement](#)
 - [no udp checksum-enforcement](#)
 - [ipv6 drop](#)
 - [no ipv6 drop](#)
 - [ipv6 decrement hop-limit](#)
 - [no ipv6 decrement hop-limit](#)
 - [ipv6 icmp](#)
 - [no ipv6 icmp](#)
 - [ipv6 site-local-unicast](#)
 - [no ipv6 site-local-unicast](#)
 - [ipv6 extension-header-check](#)
 - [no ipv6 extension-header-check](#)
 - [ipv6 extension-header-order-check](#)
 - [no ipv6 extension-header-order-check](#)
 - [ipv6 netbios-for-isatap](#)
 - [no ipv6 netbios-for-isatap](#)
 - [control-plane-flood-protection](#)
 - [no control-plane-flood-protection](#)
 - [control-plane-flood-protection-threshold](#)
 - [deregister firewall](#)
- ecli/multicast.cdl
 - [multicast](#)
 - [enable](#)
 - [no enable](#)
 - [enable-require-igmp-membership](#)
 - [no enable-require-igmp-membership](#)
 - [require-igmp-membership-timeout](#)
 - [no reception](#)
 - [reception](#)
 - [clear multicast state-entries](#)
 - [clear multicast state-entry](#)
- ecli/policy.cdl

- [no access-rule ipv4 from](#)
- [clear access-rule statistics](#)
- [access-rule ipv4 from](#)
- [access-rule ipv4 uuid](#)
- [no access-rule ipv4 uuid](#)
- [access-rule restore-defaults](#)
- [access-rules max-count](#)
- [no access-rule ipv6 from](#)
- [access-rule ipv6 from](#)
- [no access-rule ipv6 uuid](#)
- [access-rule ipv6 uuid](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [no name](#)
- [from](#)
- [to](#)
- [action](#)
- [max-connections](#)
- [priority](#)
- [no priority](#)
- [tcp timeout](#)
- [udp timeout](#)
- [fragments](#)
- [no fragments](#)
- [botnet-filter](#)
- [no botnet-filter](#)
- [comment](#)
- [no comment](#)
- [connection-limit destination](#)
- [no connection-limit destination](#)
- [connection-limit source](#)
- [no connection-limit source](#)
- [tcp urgent](#)
- [no tcp urgent](#)
- [dpi](#)
- [no dpi](#)
- [dpi-ssl](#)
- [no dpi-ssl](#)
- [redirect-unauthenticated-users-to-log-in](#)
- [no redirect-unauthenticated-users-to-log-in](#)
- [destination address](#)
- [service](#)
- [enable](#)
- [no enable](#)
- [auto-rule](#)
- [no auto-rule](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [geo-ip-filter](#)
- [no geo-ip-filter](#)
- [block country](#)
- [no block country](#)
- [block countries](#)
- [no block countries](#)
- [logging](#)
- [no logging](#)
- [sip](#)
- [no sip](#)
- [h323](#)
- [no h323](#)
- [packet-monitoring](#)
- [no packet-monitoring](#)
- [packet-dissection-filter](#)
- [no packet-dissection-filter](#)
- [management](#)
- [no management](#)
- [single-sign-on](#)
- [no single-sign-on](#)
- [block-traffic-for-single-sign-on](#)
- [no block-traffic-for-single-sign-on](#)
- [quality-of-service class-of-service](#)
- [cos-override](#)
- [no cos-override](#)
- [no quality-of-service](#)
- [quality-of-service dscp](#)
- [reflexive](#)
- [no reflexive](#)
- [schedule](#)
- [source address](#)
- [source port](#)
- [users included](#)
- [users excluded](#)
- [bandwidth-management](#)
- [bandwidth-management](#)
- [egress](#)
- [no egress](#)
- [ingress](#)
- [no ingress](#)
- [usage-tracking](#)
- [no usage-tracking](#)
- [ticket tag1](#)

- [no ticket tag1](#)
- [ticket tag2](#)
- [no ticket tag2](#)
- [ticket tag3](#)
- [no ticket tag3](#)
- [clear policy](#)
- [generate shadow-list](#)
- [ecli/ssl-control.cdl](#)
 - [ssl-control](#)
 - [enable](#)
 - [no enable](#)
 - [action](#)
 - [blacklist](#)
 - [no blacklist](#)
 - [detect ssl-v2](#)
 - [no detect ssl-v2](#)
 - [detect ssl-v3](#)
 - [no detect ssl-v3](#)
 - [detect weak-ciphers](#)
 - [no detect weak-ciphers](#)
 - [whitelist](#)
 - [no whitelist](#)
 - [detect self-signed](#)
 - [no detect self-signed](#)
 - [detect weak-digest-cert](#)
 - [no detect weak-digest-cert](#)
 - [detect expired](#)
 - [no detect expired](#)
 - [detect untrusted-ca](#)
 - [no detect untrusted-ca](#)
 - [detect tls-v1](#)
 - [no detect tls-v1](#)
 - [blacklist-certificate](#)
 - [no blacklist-certificate](#)
 - [no blacklist-certificates](#)
 - [common-name](#)
 - [whitelist-certificate](#)
 - [no whitelist-certificate](#)
 - [no whitelist-certificates](#)
 - [common-name](#)
- [ecli/tcp.cdl](#)
 - [tcp](#)
 - [enforce-strict-compliance](#)
 - [no enforce-strict-compliance](#)
 - [handshake-enforcement](#)
 - [no handshake-enforcement](#)
 - [checksum-enforcement](#)
 - [no checksum-enforcement](#)
 - [drop syn-with-data](#)
 - [no drop syn-with-data](#)
 - [drop invalid-urgent](#)
 - [no drop invalid-urgent](#)
 - [enable-handshake-timeout](#)
 - [no enable-handshake-timeout](#)
 - [handshake-timeout](#)
 - [default-connection-timeout](#)
 - [maximum-segment-lifetime](#)
 - [half-open-threshold](#)
 - [no half-open-threshold](#)
 - [maximum-half-open-connections](#)
 - [syn-flood-protection-mode](#)
 - [syn-attack-threshold](#)
 - [support-tcp-sack](#)
 - [no support-tcp-sack](#)
 - [enable-limit-mss](#)
 - [no enable-limit-mss](#)
 - [limit-mss-max](#)
 - [always-log-syn-packets](#)
 - [no always-log-syn-packets](#)
 - [proxy-connections](#)
 - [no proxy-connections](#)
 - [syn-flood-blacklisting](#)
 - [no syn-flood-blacklisting](#)
 - [blacklist-threshold](#)
 - [never-blacklist-wan](#)
 - [no never-blacklist-wan](#)
 - [always-allow-management](#)
 - [no always-allow-management](#)
 - [ddos on-wan-interfaces](#)
 - [no ddos on-wan-interfaces](#)
 - [ddos threshold](#)
 - [no ddos threshold](#)
 - [ddos filter-bypass-rate](#)
 - [no ddos filter-bypass-rate](#)
 - [ddos allow-list-timeout](#)
 - [no ddos allow-list-timeout](#)
 - [ddos always-allow-management](#)
 - [no ddos always-allow-management](#)
 - [ddos always-allow-negotiation](#)
 - [no ddos always-allow-negotiation](#)

- [clear tcp statistics](#)
- [ecli/bandwidth-object.cdl](#)
 - [no bandwidth-object](#)
 - [no bandwidth-objects](#)
 - [bandwidth-object](#)
 - [name](#)
 - [guaranteed](#)
 - [no guaranteed](#)
 - [maximum](#)
 - [priority](#)
 - [action](#)
 - [comment](#)
 - [no comment](#)
 - [per-ip-management](#)
 - [no per-ip-management](#)
- [ecli/cipher-control.cdl](#)
 - [cipher-control tls](#)
 - [cipher-control ssh](#)
 - [no cipher](#)
 - [cipher](#)
 - [no ciphers strength](#)
 - [ciphers strength](#)
 - [no key-exchange](#)
 - [key-exchange](#)
 - [no public-key](#)
 - [public-key](#)
 - [no encryption](#)
 - [encryption](#)
 - [no mac](#)
 - [mac](#)
- [ecli/udp.cdl](#)
 - [udp](#)
 - [default-connection-timeout](#)
 - [flood protection](#)
 - [no flood protection](#)
 - [flood attack-threshold](#)
 - [flood block-timeout](#)
 - [flood protected-dest-list](#)
 - [clear udp statistics](#)
- [ecli/icmp.cdl](#)
 - [icmp](#)
 - [flood protection](#)
 - [no flood protection](#)
 - [flood attack-threshold](#)
 - [flood block-timeout](#)
 - [flood protected-dest-list](#)
 - [clear icmp statistics](#)
- [ecli/dynamic-external-objects.cdl](#)
 - [dynamic-external-object](#)
 - [no dynamic-external-object](#)
 - [no dynamic-external-objects](#)
 - [type address-group](#)
 - [name](#)
 - [zone](#)
 - [fqdn](#)
 - [no fqdn](#)
 - [periodic-download](#)
 - [no periodic-download](#)
 - [protocol](#)
 - [url](#)
 - [no url](#)
 - [server](#)
 - [no server](#)
 - [login](#)
 - [no login](#)
 - [password](#)
 - [no password](#)
 - [directory](#)
 - [no directory](#)
 - [filename](#)
 - [no filename](#)
 - [clear dynamic-external-object statistics](#)
 - [download dynamic-external-object](#)
- [ecli/qos-mapping.cdl](#)
 - [qos-mapping cos](#)
 - [qos-mapping reset](#)
- [ecli/firewall_show.cdl](#)
 - [show firewall](#)
- [ecli/multicast_show.cdl](#)
 - [show multicast](#)
- [ecli/policy_show.cdl](#)
 - [show access-rule ipv4 from](#)
 - [show access-rule ipv4 uuid](#)
 - [show access-rules](#)

- [show access-rule ipv6 from](#)
 - [show access-rule ipv6 uuid](#)
- ecli/ssl-control_show.cdl
 - [show ssl-control](#)
- ecli/tcp_show.cdl
 - [show tcp](#)
- ecli/bandwidth-object_show.cdl
 - [show bandwidth-objects](#)
 - [show bandwidth-object](#)
- ecli/cipher-control_show.cdl
 - [show cipher-control tls-cipher-list](#)
 - [show cipher-control ssh](#)
- ecli/udp_show.cdl
 - [show udp](#)
 - [show udpv6](#)
- ecli/icmp_show.cdl
 - [show icmp](#)
 - [show icmpv6](#)
- ecli/dynamic-external-objects_show.cdl
 - [show dynamic-external-object](#)
 - [show dynamic-external-objects](#)
- ecli/qos-mapping_show.cdl
 - [show qos-mapping](#)
- ecli/administration.cdl
 - [administration](#)
 - [firewall-name](#)
 - [no firewall-name](#)
 - [auto-append-suffix](#)
 - [no auto-append-suffix](#)
 - [cloud-backup-enable](#)
 - [no cloud-backup-enable](#)
 - [firewall-domain-name](#)
 - [no firewall-domain-name](#)
 - [language-override](#)
 - [no language-override](#)
 - [admin name](#)
 - [admin password](#)
 - [admin one-time-password totp](#)
 - [no admin one-time-password](#)
 - [admin unbind-totp-key](#)
 - [wireless-lan](#)
 - [no wireless-lan](#)
 - [ipv6](#)
 - [no ipv6](#)
 - [password aging](#)
 - [no password aging](#)
 - [password last-changed](#)
 - [no password last-changed](#)
 - [password uniqueness](#)
 - [no password uniqueness](#)
 - [password enforce-character-difference](#)
 - [no password enforce-character-difference](#)
 - [password minimum-length](#)
 - [password complexity alpha-and-numeric-and-symbols](#)
 - [password complexity alpha-and-numeric](#)
 - [no password complexity](#)
 - [password complexity type](#)
 - [password complexity upper-case](#)
 - [password complexity lower-case](#)
 - [password complexity digital](#)
 - [password complexity symbolic](#)
 - [password constraints-apply-to](#)
 - [no password constraints-apply-to](#)
 - [idle-logout-time](#)
 - [user-lockout](#)
 - [no user-lockout](#)
 - [local-user-lockout](#)
 - [no local-user-lockout](#)
 - [log-without-lockout](#)
 - [no log-without-lockout](#)
 - [max-login-attempts-cli](#)
 - [admin preempt-action](#)
 - [admin preempt-inactivity-timeout](#)
 - [inter-admin-messaging](#)
 - [no inter-admin-messaging](#)
 - [multiple-admin](#)
 - [no multiple-admin](#)
 - [enhanced-audit-logging](#)
 - [no enhanced-audit-logging](#)
 - [wireless-controller-mode](#)
 - [web-management allow-http](#)
 - [no web-management allow-http](#)
 - [http-port](#)
 - [https-port](#)

- [web-management certificate](#)
- [web-management cert-common-name](#)
- [no web-management cert-common-name](#)
- [web-management client-certificate-check](#)
- [no web-management client-certificate-check](#)
- [web-management client-certificate-cache](#)
- [no web-management client-certificate-cache](#)
- [web-management user-name-field](#)
- [web-management client-certificate-issuer](#)
- [web-management cac-user-group-retrieve](#)
- [web-management ocsp-check](#)
- [no web-management ocsp-check](#)
- [web-management ocsp-periodic-check enable](#)
- [no web-management ocsp-periodic-check enable](#)
- [web-management ocsp_check_interval](#)
- [web-management default-table-size](#)
- [web-management refresh-interval](#)
- [web-management tooltip](#)
- [no web-management tooltip](#)
- [web-management certification-periodic-expiration-check](#)
- [no web-management certification-periodic-expiration-check](#)
- [web-management certification-expiration-interval](#)
- [uuid all](#)
- [no uuid all](#)
- [uuid address-objects](#)
- [no uuid address-objects](#)
- [uuid service-objects](#)
- [no uuid service-objects](#)
- [uuid user-objects](#)
- [no uuid user-objects](#)
- [uuid schedule-objects](#)
- [no uuid schedule-objects](#)
- [uuid zone-objects](#)
- [no uuid zone-objects](#)
- [uuid access-rules](#)
- [no uuid access-rules](#)
- [uuid nat-policy](#)
- [no uuid nat-policy](#)
- [uuid routing-policy](#)
- [no uuid routing-policy](#)
- [uuid content-filter-objects](#)
- [no uuid content-filter-objects](#)
- [uuid content-filter-policies](#)
- [no uuid content-filter-policies](#)
- [uuid network-monitor-policy](#)
- [no uuid network-monitor-policy](#)
- [uuid sdwan-performance-probes](#)
- [no uuid sdwan-performance-probes](#)
- [dashboard-as-starting-page](#)
- [no dashboard-as-starting-page](#)
- [tls-and-above](#)
- [no tls-and-above](#)
- [out-of-band-management](#)
- [no out-of-band-management](#)
- [gms-management](#)
- [no gms-management](#)
- [host-name](#)
- [no host-name](#)
- [syslog-server-port](#)
- [no syslog-server-port](#)
- [heartbeat-status-only](#)
- [no heartbeat-status-only](#)
- [behind-nat-device](#)
- [no behind-nat-device](#)
- [spi](#)
- [no spi](#)
- [encryption-type](#)
- [encryption-key](#)
- [authentication-key](#)
- [reporting-server](#)
- [no reporting-server](#)
- [sonicos-api](#)
- [enable](#)
- [no enable](#)
- [digest](#)
- [no digest](#)
- [sha256-digest](#)
- [no sha256-digest](#)
- [md5-digest](#)
- [no md5-digest](#)
- [integrity-protection](#)
- [no integrity-protection](#)
- [session-variant](#)
- [no session-variant](#)
- [chap](#)
- [no chap](#)
- [basic](#)
- [no basic](#)
- [public-key](#)
- [no public-key](#)
- [rsa-key-size](#)
- [rsa-padding-type](#)

- [oeap-hash-mode](#)
- [oeap-mask-method](#)
- [session-security](#)
- [no session-security](#)
- [max-nonce](#)
- [two-factor-bearer-token](#)
- [no two-factor-bearer-token](#)
- [auto-commit](#)
- [no auto-commit](#)
- [log](#)
- [no log](#)
- [compress-response-during-transmission](#)
- [no compress-response-during-transmission](#)
- [hateoas](#)
- [no hateoas](#)
- [force-through](#)
- [regenerate-certificate](#)
- [ecli/snmp.cdl](#)
 - [snmp](#)
 - [enable](#)
 - [no enable](#)
 - [system-name](#)
 - [no system-name](#)
 - [system-contact](#)
 - [no system-contact](#)
 - [system-location](#)
 - [no system-location](#)
 - [asset-number](#)
 - [no asset-number](#)
 - [get-community-name](#)
 - [no get-community-name](#)
 - [trap-community-name](#)
 - [no trap-community-name](#)
 - [host-1](#)
 - [no host-1](#)
 - [host-2](#)
 - [no host-2](#)
 - [host-3](#)
 - [no host-3](#)
 - [host-4](#)
 - [no host-4](#)
 - [snmp3 mandatory](#)
 - [no snmp3 mandatory](#)
 - [snmp3 engine-id](#)
 - [snmp3 increase-subsystem-priority](#)
 - [no snmp3 increase-subsystem-priority](#)
 - [view](#)
 - [no view](#)
 - [group](#)
 - [no group](#)
 - [name](#)
 - [user](#)
 - [no user](#)
 - [no users](#)
 - [name](#)
 - [security-level](#)
 - [no security-level](#)
 - [authentication](#)
 - [no authentication](#)
 - [encryption](#)
 - [no encryption](#)
 - [group](#)
 - [no group](#)
 - [access](#)
 - [no access](#)
 - [no accesses](#)
 - [name](#)
 - [read-view](#)
 - [master-group](#)
 - [security-level](#)
 - [no security-level](#)
- [ecli/export.cdl](#)
 - [export core-dump](#)
 - [export swarm](#)
 - [export current-config](#)
 - [export pending-config](#)
 - [export tech-support-report](#)
 - [export ssoauth-log](#)
 - [export-and-reset ssoauth-log](#)
 - [export trace-log](#)
 - [export console-logs](#)
 - [export safe-mode-logs](#)
 - [export object](#)
 - [export policy](#)
 - [export shadow-rule-list](#)
 - [export firmware](#)
- [ecli/firmware.cdl](#)
 - [firmware auto](#)
 - [no firmware auto](#)

- [ftp send-tsr](#)
- [no ftp send-tsr](#)
- [ftp send-settings](#)
- [no ftp send-settings](#)
- [ftp server](#)
- [no ftp server](#)
- [ftp user](#)
- [no ftp user](#)
- [ftp password](#)
- [no ftp password](#)
- [ftp directory](#)
- [no ftp directory](#)
- [no upload-firmware](#)
- [no local-backups](#)
- [local-backups boot](#)
- [local-backup create](#)
- [no local-backup name](#)
- [local-backup comment](#)
- [no local-backup comment](#)
- [local-backup retain](#)
- [no local-backup retain](#)
- [local-backup gold](#)
- [no local-backup gold](#)
- [no cloud-backups](#)
- [cloud-backup create](#)
- [no cloud-backup name](#)
- [cloud-backup retain](#)
- [no cloud-backup retain](#)
- [no cloud-backup comment](#)
- [cloud-backup comment](#)
- [cloud-backup gold](#)
- [no cloud-backup gold](#)
- [auto-upgrade](#)
- [no auto-upgrade](#)
- [ecli/import.cdl](#)
 - [import firmware](#)
 - [import cli](#)
 - [import exp](#)
 - [get](#)
 - [put](#)
 - [post](#)
 - [delete](#)
 - [import file](#)
- [ecli/system.cdl](#)
 - [restart](#)
 - [safemode](#)
 - [restore-defaults](#)
 - [boot](#)
 - [sysfile](#)
 - [storage-dev](#)
 - [logs-on-storage](#)
 - [no logs-on-storage](#)
 - [clear sysfile](#)
 - [no connection caches](#)
 - [no connection cache](#)
 - [export sysfile](#)
- [ecli/time.cdl](#)
 - [time](#)
 - [time](#)
 - [date](#)
 - [time-zone](#)
 - [use-ntp](#)
 - [no use-ntp](#)
 - [daylight-savings](#)
 - [no daylight-savings](#)
 - [universal](#)
 - [no universal](#)
 - [international-format](#)
 - [no international-format](#)
 - [only-custom-ntp](#)
 - [no only-custom-ntp](#)
 - [ntp-update-interval](#)
 - [ntp-server](#)
 - [no ntp-server](#)
 - [no ntp-servers](#)
 - [name](#)
 - [no-auth](#)
 - [md5](#)
- [ecli/license.cdl](#)
 - [license](#)
 - [synchronize](#)
 - [lmsync](#)
 - [upgrade](#)
 - [register-code](#)
- [ecli/ssh-server.cdl](#)
 - [ssh server](#)
 - [port](#)
 - [keygen](#)

- [restart](#)
 - [enable](#)
 - [terminate](#)
 - [kill session](#)
 - [kill sessions](#)
- ecli/fips.cdl
 - [fips](#)
 - [no fips](#)
- ecli/ndpp.cdl
 - [ndpp](#)
 - [no ndpp](#)
- ecli/administration_show.cdl
 - [show administration](#)
- ecli/snmp_show.cdl
 - [show snmp](#)
- ecli/firmware_show.cdl
 - [show firmware](#)
 - [show ftp](#)
- ecli/status_show.cdl
 - [show status](#)
- ecli/system_show.cdl
 - [show sysfile](#)
- ecli/time_show.cdl
 - [show time](#)
- ecli/version_show.cdl
 - [show version](#)
- ecli/license_show.cdl
 - [show license](#)
- ecli/ssh-server_show.cdl
 - [show ssh server](#)
- ecli/fips_show.cdl
 - [show fips](#)
- ecli/ndpp_show.cdl
 - [show ndpp](#)
- ecli/user-auth.cdl
 - [user authentication](#)
 - [auth-method](#)
 - [sso-method](#)
 - [no sso-method](#)
 - [case-sensitive-names](#)
 - [no case-sensitive-names](#)
 - [login-uniqueness](#)
 - [no login-uniqueness](#)
 - [relogin-after-password-change](#)
 - [no relogin-after-password-change](#)
 - [display-login-info](#)
 - [no display-login-info](#)
 - [one-time-password-constraints](#)
 - [no one-time-password-constraints](#)
 - [one-time-password format](#)
 - [one-time-password length](#)
 - [one-time-password email-format](#)
 - [auth-page-timeout](#)
 - [no auth-page-timeout](#)
 - [browser-redirect-via](#)
 - [redirect-to-login-page](#)
 - [http-redirect-after-login](#)
 - [no http-redirect-after-login](#)
 - [radius-chap-http-login](#)
 - [no radius-chap-http-login](#)
 - [redirect-external-page](#)
 - [no redirect-external-page](#)
 - [combined-login](#)
 - [no combined-login](#)
 - [auth-page-as-frame](#)
 - [no auth-page-as-frame](#)
 - [policy-banner-before-login](#)
 - [no policy-banner-before-login](#)
 - [policy-banner](#)
 - [no policy-banner](#)
 - [inactivity-timeout](#)
 - [prevent-inactivity-logout service](#)
 - [no prevent-inactivity-logout service](#)
 - [log-user-name](#)
 - [no log-user-name](#)
 - [user-connections-logout](#)
 - [inactive-user](#)
 - [no inactive-user](#)
 - [age-out](#)
 - [web-login-session-limit](#)

- [no web-login-session-limit](#)
- [show-user-status-window](#)
- [no show-user-status-window](#)
- [status-window-heartbeat](#)
- [disconnected-user-detect](#)
- [no disconnected-user-detect](#)
- [open-in-same-window](#)
- [no open-in-same-window](#)
- [rule-auth-bypass-http-url](#)
- [no rule-auth-bypass-http-url](#)
- [acceptable-use-policy](#)
- [window-size](#)
- [scroll-bars](#)
- [no scroll-bars](#)
- [content](#)
- [no content](#)
- [aup-on-zones](#)
- [no aup-on-zones](#)
- [customize-login-page](#)
- [no customize-login-page](#)
- [track-traffic](#)
- [ecli/user-local.cdl](#)
 - [user local](#)
 - [apply-password-constraints](#)
 - [no apply-password-constraints](#)
 - [prune-on-expiry](#)
 - [no prune-on-expiry](#)
 - [inactivity-timeout](#)
 - [no inactivity-timeout](#)
 - [prune-on-inactive](#)
 - [no prune-on-inactive](#)
 - [domain-name-display-format](#)
 - [user](#)
 - [no user](#)
 - [no users](#)
 - [group](#)
 - [no group](#)
 - [no groups](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [domain](#)
 - [no domain](#)
 - [comment](#)
 - [no comment](#)
 - [password](#)
 - [no password](#)
 - [force-password-change](#)
 - [no force-password-change](#)
 - [expiration](#)
 - [account-lifetime](#)
 - [no account-lifetime](#)
 - [prune-on-expiry](#)
 - [no prune-on-expiry](#)
 - [one-time-password](#)
 - [no one-time-password](#)
 - [unbind-totp-key](#)
 - [email-address](#)
 - [no email-address](#)
 - [vpn-client-access](#)
 - [no vpn-client-access](#)
 - [guest-login-uniqueness](#)
 - [no guest-login-uniqueness](#)
 - [guest-idle-timeout](#)
 - [no guest-idle-timeout](#)
 - [no quota-cycle](#)
 - [quota-cycle](#)
 - [session-lifetime](#)
 - [no session-lifetime](#)
 - [limit](#)
 - [no limit](#)
 - [member-of](#)
 - [no member-of](#)
 - [no members-of](#)
 - [name](#)
 - [domain](#)
 - [no domain](#)
 - [comment](#)
 - [no comment](#)
 - [ldap-location](#)
 - [no ldap-location](#)
 - [memberships-by-ldap-location](#)
 - [no memberships-by-ldap-location](#)
 - [refresh-from-ldap-server](#)
 - [one-time-password](#)
 - [no one-time-password](#)
 - [to-management-on-login](#)
 - [no to-management-on-login](#)
 - [read-only-restriction](#)
 - [no read-only-restriction](#)
 - [vpn-client-access](#)

- [no vpn-client-access](#)
- [member](#)
- [no member](#)
- [no members](#)
- [uuid](#)
- [no uuid](#)
- [bookmark](#)
- [no bookmark](#)
- [no bookmarks](#)
- [name](#)
- [host](#)
- [no host](#)
- [service](#)
- [screen-size](#)
- [colors](#)
- [application-path](#)
- [no application-path](#)
- [start-in-folder](#)
- [no start-in-folder](#)
- [automatic-login](#)
- [no automatic-login](#)
- [redirect-clipboard](#)
- [no redirect-clipboard](#)
- [redirect-audio](#)
- [no redirect-audio](#)
- [auto-reconnection](#)
- [no auto-reconnection](#)
- [desktop-background](#)
- [no desktop-background](#)
- [window-drag](#)
- [no window-drag](#)
- [animation](#)
- [no animation](#)
- [view-only](#)
- [no view-only](#)
- [share-desktop](#)
- [no share-desktop](#)
- [automatic-accept-host-key](#)
- [no automatic-accept-host-key](#)
- [display-on-mobile](#)
- [no display-on-mobile](#)
- [bookmark](#)
- [no bookmark](#)
- [no bookmarks](#)
- [name](#)
- [host](#)
- [no host](#)
- [service](#)
- [screen-size](#)
- [colors](#)
- [application-path](#)
- [no application-path](#)
- [start-in-folder](#)
- [no start-in-folder](#)
- [automatic-login](#)
- [no automatic-login](#)
- [redirect-clipboard](#)
- [no redirect-clipboard](#)
- [redirect-audio](#)
- [no redirect-audio](#)
- [auto-reconnection](#)
- [no auto-reconnection](#)
- [desktop-background](#)
- [no desktop-background](#)
- [window-drag](#)
- [no window-drag](#)
- [animation](#)
- [no animation](#)
- [view-only](#)
- [no view-only](#)
- [share-desktop](#)
- [no share-desktop](#)
- [automatic-accept-host-key](#)
- [no automatic-accept-host-key](#)
- [display-on-mobile](#)
- [no display-on-mobile](#)
- [unbind-totp-key](#)
- [ecli/user-mgmt.cdl](#)
 - [kill-user name](#)
 - [kill-user at](#)
 - [kill-user inactive at](#)
 - [unlock-ip](#)
 - [unlock-account](#)
 - [user management](#)
 - [include](#)
 - [no include](#)
 - [send-message](#)
- [ecli/user-radius.cdl](#)
 - [user radius](#)
 - [clear user radius statistics](#)

- [local-users-only](#)
- [no local-users-only](#)
- [default-user-group](#)
- [no default-user-group](#)
- [timeout](#)
- [retries](#)
- [periodic-check-server](#)
- [no periodic-check-server](#)
- [mschapv2-mode](#)
- [no mschapv2-mode](#)
- [user-group-mechanism](#)
- [server](#)
- [no server](#)
- [no servers](#)
- [enable](#)
- [no enable](#)
- [host](#)
- [port](#)
- [shared-secret](#)
- [no shared-secret](#)
- [send-through-vpn-tunnel](#)
- [no send-through-vpn-tunnel](#)
- [user-name-format](#)
- [test](#)
- [accounting](#)
- [server](#)
- [no server](#)
- [no servers](#)
- [enable](#)
- [no enable](#)
- [host](#)
- [port](#)
- [shared-secret](#)
- [no shared-secret](#)
- [user-name-format](#)
- [test](#)
- [timeout](#)
- [retries](#)
- [data](#)
- [no data](#)
- [include](#)
- [interim-updates](#)
- [no interim-updates](#)
- [ecli/user-ldap.cdl](#)
 - [user ldap](#)
 - [clear user ldap statistics](#)
 - [protocol-version](#)
 - [require-valid-certificate](#)
 - [no require-valid-certificate](#)
 - [local-tls-certificate](#)
 - [no local-tls-certificate](#)
 - [allow-referrals](#)
 - [no allow-referrals](#)
 - [allow-references](#)
 - [no allow-references](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [default-user-group](#)
 - [no default-user-group](#)
 - [check-deleted-groups-method](#)
 - [mirror-user-groups](#)
 - [no mirror-user-groups](#)
 - [exclude-tree](#)
 - [no exclude-tree](#)
 - [relay](#)
 - [enable](#)
 - [no enable](#)
 - [clients-connect](#)
 - [no clients-connect](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [legacy-user-group](#)
 - [no legacy-user-group](#)
 - [server](#)
 - [no server](#)
 - [no servers](#)
 - [save dynamic-secondary](#)
 - [no dynamic-server](#)
 - [enable](#)
 - [no enable](#)
 - [host](#)
 - [role](#)
 - [port](#)
 - [timeout](#)
 - [use-tls](#)
 - [no use-tls](#)
 - [send-start-tls-request](#)
 - [no send-start-tls-request](#)
 - [backup-for](#)
 - [no backup-for](#)
 - [same-bind-credentials](#)

- [no same-bind-credentials](#)
- [schema](#)
- [read-from-server auto-configure](#)
- [read-from-server display](#)
- [user-class](#)
- [user-attribute](#)
- [no user-attribute](#)
- [user-group-class](#)
- [user-group-attribute](#)
- [no user-group-attribute](#)
- [directory](#)
- [read-trees-from-server](#)
- [primary-domain](#)
- [no primary-domain](#)
- [users-tree](#)
- [no users-tree](#)
- [no users-trees](#)
- [user-groups-tree](#)
- [no user-groups-tree](#)
- [no user-groups-trees](#)
- [bind](#)
- [bind-password](#)
- [no bind-password](#)
- [referred-bind-with-account](#)
- [test](#)
- [import](#)
- [ecli/user-sso.cdl](#)
 - [user sso](#)
 - [clear user sso statistics](#)
 - [method](#)
 - [no method](#)
 - [next-agent-on-no-name](#)
 - [no next-agent-on-no-name](#)
 - [block-traffic](#)
 - [no block-traffic](#)
 - [including-for-access-rules](#)
 - [no including-for-access-rules](#)
 - [sync-all-agents-user-db](#)
 - [no sync-all-agents-user-db](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [non-domain-limited-access](#)
 - [no non-domain-limited-access](#)
 - [probe](#)
 - [no probe](#)
 - [user-group-mechanism](#)
 - [poll rate](#)
 - [poll same-agent](#)
 - [no poll same-agent](#)
 - [hold-time after-failure](#)
 - [hold-time after-no-user](#)
 - [ramp-up rate](#)
 - [no ramp-up](#)
 - [user-domain-name](#)
 - [windows-service-user-name](#)
 - [no windows-service-user-name](#)
 - [no windows-service-user-names](#)
 - [name](#)
 - [security-service-bypass address](#)
 - [no security-service-bypass address](#)
 - [security-service-bypass service](#)
 - [no security-service-bypass service](#)
 - [address](#)
 - [service](#)
 - [type](#)
 - [log-user-name](#)
 - [no log-user-name](#)
 - [dummy-user](#)
 - [no dummy-user](#)
 - [enforce-on-zone](#)
 - [no enforce-on-zone](#)
 - [bypass-policy](#)
 - [no bypass-policy](#)
 - [tsa-services-bypass](#)
 - [no tsa-services-bypass](#)
 - [authentication-domain](#)
 - [redirect-browser](#)
 - [retries-on-failure](#)
 - [poll users](#)
 - [forward-lanman](#)
 - [no forward-lanman](#)
 - [radius-accounting-port](#)
 - [radius-acct-lookup-mechanism](#)
 - [switch-over-time](#)
 - [no switch-over-time](#)
 - [ignore-transition-message](#)
 - [no ignore-transition-message](#)
 - [ignore-addr](#)
 - [include-addr](#)
 - [radius-user-name-exclusion](#)
 - [no radius-user-name-exclusion](#)

- [no radius-user-name-exclusions](#)
- [name](#)
- [type](#)
- [agent](#)
- [no agent](#)
- [no agents](#)
- [host](#)
- [port](#)
- [enable](#)
- [no enable](#)
- [timeout](#)
- [retries](#)
- [no shared-key](#)
- [shared-key](#)
- [max-requests](#)
- [terminal-services-agent](#)
- [no terminal-services-agent](#)
- [no terminal-services-agents](#)
- [host](#)
- [port](#)
- [enable](#)
- [no enable](#)
- [no shared-key](#)
- [shared-key](#)
- [radius-accounting-client](#)
- [no radius-accounting-client](#)
- [no radius-accounting-clients](#)
- [host](#)
- [shared-secret](#)
- [no shared-secret](#)
- [user-name-format](#)
- [custom-format-components component1](#)
- [custom-format-components component2](#)
- [custom-format-components component3](#)
- [missing-domain](#)
- [log-user-out-if-no-interim](#)
- [no log-user-out-if-no-interim](#)
- [log-user-out-timeout](#)
- [no log-user-out-timeout](#)
- [server](#)
- [no server](#)
- [proxy-forward timeout](#)
- [proxy-forward retries](#)
- [proxy-forward type](#)
- [consistent-domain-name](#)
- [no consistent-domain-name](#)
- [no consistent-domain-names](#)
- [dn](#)
- [name](#)
- [no name](#)
- [test](#)
- [third-party-api](#)
- [enable](#)
- [no enable](#)
- [https-port](#)
- [client](#)
- [no client](#)
- [no clients](#)
- [host](#)
- [enable](#)
- [no enable](#)
- [authentication-type](#)
- [shared-secret](#)
- [no shared-secret](#)
- [security-level](#)
- [replay-prevention](#)
- [no replay-prevention](#)
- [origin-restriction](#)
- [no origin-restriction](#)
- [persistent-connections](#)
- [no persistent-connections](#)
- [capture-client](#)
- [enable](#)
- [no enable](#)
- [ecli/user-guest.cdl](#)
 - [user guest](#)
 - [profile](#)
 - [no profile](#)
 - [user](#)
 - [generate](#)
 - [num](#)
 - [no user](#)
 - [no users](#)
 - [show-guest-status-window](#)
 - [no show-guest-status-window](#)
 - [export guest-accounts](#)
 - [logout guest](#)
 - [logout guests](#)
 - [name](#)
 - [generate](#)
 - [no generate](#)

- [name-prefix](#)
- [comment](#)
- [no comment](#)
- [enable](#)
- [no enable](#)
- [activate-on-login](#)
- [no activate-on-login](#)
- [login-uniqueness](#)
- [no login-uniqueness](#)
- [prune-on-expiry](#)
- [no prune-on-expiry](#)
- [account-lifetime](#)
- [no quota-cycle](#)
- [quota-cycle](#)
- [session-lifetime](#)
- [idle-timeout](#)
- [limit](#)
- [no limit](#)
- [name](#)
- [uuid](#)
- [no uuid](#)
- [generate](#)
- [profile](#)
- [comment](#)
- [no comment](#)
- [password](#)
- [no password](#)
- [enable](#)
- [no enable](#)
- [activate-on-login](#)
- [no activate-on-login](#)
- [login-uniqueness](#)
- [no login-uniqueness](#)
- [prune-on-expiry](#)
- [no prune-on-expiry](#)
- [account-lifetime](#)
- [no quota-cycle](#)
- [quota-cycle](#)
- [session-lifetime](#)
- [no session-lifetime](#)
- [idle-timeout](#)
- [limit](#)
- [no limit](#)
- [ecli/user-tacacs.cdl](#)
 - [user tacacs](#)
 - [local-users-only](#)
 - [no local-users-only](#)
 - [user-group-mechanism](#)
 - [default-user-group](#)
 - [no default-user-group](#)
 - [timeout](#)
 - [retries](#)
 - [no retries](#)
 - [single-connect](#)
 - [no single-connect](#)
 - [periodic-check](#)
 - [no periodic-check](#)
 - [server](#)
 - [no server](#)
 - [no servers](#)
 - [host](#)
 - [port](#)
 - [enable](#)
 - [no enable](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [through-vpn](#)
 - [no through-vpn](#)
 - [test](#)
 - [accounting](#)
 - [server](#)
 - [no server](#)
 - [no servers](#)
 - [enable](#)
 - [no enable](#)
 - [host](#)
 - [port](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [test](#)
 - [timeout](#)
 - [retries](#)
 - [no retries](#)
 - [single-connect](#)
 - [no single-connect](#)
 - [packet-encrypted](#)
 - [no packet-encrypted](#)
 - [data](#)
 - [no data](#)
 - [include](#)
 - [watchdog-messages](#)

- [no watchdog-messages](#)
- ecli/user-auth_show.cdl
 - [show user authentication](#)
- ecli/user-local_show.cdl
 - [show user local](#)
- ecli/user-mgmt_show.cdl
 - [show user status](#)
 - [show user statistics](#)
 - [show user management](#)
 - [show user sessions statistics](#)
- ecli/user-radius_show.cdl
 - [show user radius](#)
- ecli/user-ldap_show.cdl
 - [show user ldap](#)
- ecli/user-sso_show.cdl
 - [show user sso](#)
- ecli/user-guest_show.cdl
 - [show user guest](#)
- ecli/user-tacacs_show.cdl
 - [show user tacacs](#)
- ecli/appflow.cdl
 - [appflow](#)
 - [clear flow-reporting statistics](#)
 - [default](#)
 - [report connections](#)
 - [real-time data-collection](#)
 - [no real-time data-collection](#)
 - [real-time collect-for](#)
 - [no real-time collect-for](#)
 - [aggregate data-collection](#)
 - [no aggregate data-collection](#)
 - [aggregate collect-for](#)
 - [no aggregate collect-for](#)
 - [flows-to local-collector](#)
 - [no flows-to local-collector](#)
 - [report dropped](#)
 - [no report dropped](#)
 - [report stack](#)
 - [no report stack](#)
 - [include-url-types](#)
 - [no include-url-types](#)
 - [geo-ip-resolution](#)
 - [no geo-ip-resolution](#)
 - [report ipv6-flows](#)
 - [no report ipv6-flows](#)
 - [gmsflow-server](#)
 - [flows](#)
 - [no flows](#)
 - [real-time](#)
 - [no real-time](#)
 - [system-logs](#)
 - [no system-logs](#)
 - [report open](#)
 - [no report open](#)
 - [report close](#)
 - [no report close](#)
 - [report update](#)
 - [no report update](#)
 - [reporting-format](#)
 - [dynamic-flows](#)
 - [no dynamic-flows](#)
 - [mode](#)
 - [auto-synchronize](#)
 - [no auto-synchronize](#)
 - [advanced-mode](#)
 - [load-balancing-mode](#)
 - [server-ip](#)
 - [server ip](#)
 - [no server ip](#)
 - [server address](#)
 - [vpn-source-ip](#)
 - [no vpn-source-ip](#)
 - [communication-timeout](#)
 - [synchronize](#)
 - [synchronize-logs](#)
 - [test-connectivity](#)
 - [server-2-ip](#)
 - [server ip](#)
 - [no server ip](#)
 - [server address](#)
 - [vpn-source-ip](#)
 - [no vpn-source-ip](#)
 - [communication-timeout](#)
 - [synchronize](#)

- [synchronize-logs](#)
- [test-connectivity](#)
- [sfr-mailing](#)
- [send-email](#)
- [no send-email](#)
- [smtp-server-host](#)
- [no smtp-server-host](#)
- [report-to-email](#)
- [no report-to-email](#)
- [report-from-email](#)
- [no report-from-email](#)
- [smtp-server-port](#)
- [security-method](#)
- [no security-method](#)
- [smtp-auth](#)
- [no smtp-auth](#)
- [smtp-user](#)
- [no smtp-user](#)
- [smtp-pass](#)
- [no smtp-pass](#)
- [pop-before-smtp](#)
- [no pop-before-smtp](#)
- [pop-server-address](#)
- [no pop-server-address](#)
- [pop-username](#)
- [no pop-username](#)
- [pop-pass](#)
- [no pop-pass](#)
- [test-email](#)
- [appflow-server](#)
- [flows](#)
- [no flows](#)
- [real-time](#)
- [no real-time](#)
- [system-logs](#)
- [no system-logs](#)
- [report open](#)
- [no report open](#)
- [report close](#)
- [no report close](#)
- [report update](#)
- [no report update](#)
- [dynamic-flows](#)
- [no dynamic-flows](#)
- [keep-alive](#)
- [no keep-alive](#)
- [mode](#)
- [auto-synchronize](#)
- [no auto-synchronize](#)
- [advanced-mode](#)
- [load-balancing-mode](#)
- [server-ip](#)
- [server ip](#)
- [no server ip](#)
- [server address](#)
- [vpn-source-ip](#)
- [no vpn-source-ip](#)
- [max-flows](#)
- [communication-timeout](#)
- [firewall-name](#)
- [passphrase](#)
- [no passphrase](#)
- [synchronize](#)
- [synchronize-logs](#)
- [test-connectivity](#)
- [flush server](#)
- [flush servers](#)
- [discover](#)
- [server-2-ip](#)
- [server ip](#)
- [no server ip](#)
- [server address](#)
- [vpn-source-ip](#)
- [no vpn-source-ip](#)
- [max-flows](#)
- [communication-timeout](#)
- [firewall-name](#)
- [passphrase](#)
- [no passphrase](#)
- [synchronize](#)
- [synchronize-logs](#)
- [test-connectivity](#)
- [external-collector](#)
- [flows](#)
- [no flows](#)
- [reporting-format](#)
- [no server ip](#)
- [server ip](#)
- [server address](#)
- [vpn-source-ip](#)
- [no vpn-source-ip](#)
- [port](#)

- [send templates](#)
- [no send templates](#)
- [send static-flows](#)
- [no send static-flows](#)
- [static-flows](#)
- [no static-flows](#)
- [dynamic-flows](#)
- [no dynamic-flows](#)
- [ipfix-reports](#)
- [no ipfix-reports](#)
- [report open](#)
- [no report open](#)
- [report close](#)
- [no report close](#)
- [report active-timeout](#)
- [no report active-timeout](#)
- [report kilobytes-exchanged](#)
- [no report kilobytes-exchanged](#)
- [report update](#)
- [no report update](#)
- [generate all-templates](#)
- [generate static-appflow-data](#)
- [send-all-entries](#)
- [cta-report](#)
- [no cta-report](#)
- [reset appflow-report](#)
- [ecli/appflow_show.cdl](#)
 - [show appflow](#)
- [ecli/certificate.cdl](#)
 - [certificates](#)
 - [export signing-request](#)
 - [export cert-key-pair](#)
 - [import cert-key-pair](#)
 - [import ca-cert](#)
 - [import signed-cert](#)
 - [import crl](#)
 - [no certificate](#)
 - [no ca-certificate](#)
 - [no certificates](#)
 - [generate-signing-request](#)
 - [no enrollment](#)
 - [scep](#)
 - [alias](#)
 - [distinguished-name element1](#)
 - [distinguished-name element2](#)
 - [distinguished-name element3](#)
 - [distinguished-name element4](#)
 - [distinguished-name element5](#)
 - [distinguished-name element6](#)
 - [distinguished-name element7](#)
 - [distinguished-name element8](#)
 - [alternate-name](#)
 - [signature-algorithm](#)
 - [key.type](#)
 - [key.size](#)
 - [generate](#)
 - [signing-request](#)
 - [ca.url](#)
 - [challenge-password](#)
 - [request-count](#)
 - [polling-interval](#)
 - [max-polling-time](#)
 - [scep](#)
- [ecli/certificate_show.cdl](#)
 - [show certificates](#)
 - [show certificate](#)
- [ecli/log.cdl](#)
 - [export log](#)
 - [clear log](#)
 - [log-action email](#)
 - [log display](#)
 - [log event](#)
 - [log group](#)
 - [log category](#)
 - [log categories](#)
 - [log syslog](#)
 - [log automation](#)
 - [log name-resolution](#)
 - [log reports](#)
 - [log viewpoint](#)
 - [log analyzer](#)
 - [save-template](#)
 - [import-template](#)
 - [reset event-count](#)
 - [custom-template-description](#)
 - [no custom-template-description](#)
 - [logging-level](#)
 - [alert-level](#)
 - [global-category-attribute](#)

- [priority-level](#)
- [log-monitor](#)
- [no log-monitor](#)
- [email-alert](#)
- [no email-alert](#)
- [syslog](#)
- [no syslog](#)
- [event-profile](#)
- [ipfix](#)
- [no ipfix](#)
- [log-digest](#)
- [no log-digest](#)
- [color](#)
- [log-email](#)
- [no log-email](#)
- [alert-email](#)
- [no alert-email](#)
- [name](#)
- [id](#)
- [priority-level](#)
- [log-monitor](#)
- [no log-monitor](#)
- [email-alert](#)
- [no email-alert](#)
- [syslog](#)
- [no syslog](#)
- [event-profile](#)
- [log view option](#)
- [no log view option](#)
- [ipfix](#)
- [no ipfix](#)
- [log-digest](#)
- [no log-digest](#)
- [color](#)
- [log-email](#)
- [no log-email](#)
- [alert-email](#)
- [no alert-email](#)
- [category](#)
- [priority-level](#)
- [log-monitor](#)
- [no log-monitor](#)
- [email-alert](#)
- [no email-alert](#)
- [syslog](#)
- [no syslog](#)
- [event-profile](#)
- [ipfix](#)
- [no ipfix](#)
- [log-digest](#)
- [no log-digest](#)
- [color](#)
- [alert-email](#)
- [no alert-email](#)
- [group](#)
- [priority-level](#)
- [log-monitor](#)
- [no log-monitor](#)
- [email-alert](#)
- [no email-alert](#)
- [syslog](#)
- [no syslog](#)
- [event-profile syslog-server-profile](#)
- [ipfix](#)
- [no ipfix](#)
- [log-digest](#)
- [no log-digest](#)
- [color](#)
- [alert-email](#)
- [no alert-email](#)
- [facility](#)
- [format](#)
- [id](#)
- [event-rate-limiting](#)
- [no event-rate-limiting](#)
- [data-rate-limiting](#)
- [no data-rate-limiting](#)
- [enhanced general](#)
- [no enhanced general](#)
- [enhanced interface](#)
- [no enhanced interface](#)
- [enhanced protocol](#)
- [no enhanced protocol](#)
- [enhanced connection](#)
- [no enhanced connection](#)
- [enhanced application](#)
- [no enhanced application](#)
- [enhanced others](#)
- [no enhanced others](#)
- [arcsight general](#)
- [no arcsight general](#)
- [arcsight interface](#)

- [no arcsight interface](#)
- [arcsight protocol](#)
- [no arcsight protocol](#)
- [arcsight connection](#)
- [no arcsight connection](#)
- [arcsight application](#)
- [no arcsight application](#)
- [arcsight others](#)
- [no arcsight others](#)
- [ndpp](#)
- [no ndpp](#)
- [type](#)
- [facility](#)
- [format](#)
- [id](#)
- [event-rate-limiting](#)
- [no event-rate-limiting](#)
- [data-rate-limiting](#)
- [no data-rate-limiting](#)
- [enabled](#)
- [no enabled](#)
- [no syslog-servers](#)
- [enable servers](#)
- [no enable servers](#)
- [server address](#)
- [no server address](#)
- [no servers](#)
- [profile](#)
- [no profile](#)
- [address](#)
- [port](#)
- [no port](#)
- [outbound-interface](#)
- [no outbound-interface](#)
- [local-interface](#)
- [no local-interface](#)
- [email-address](#)
- [no email-address](#)
- [send-log](#)
- [email-format-log](#)
- [send-audit](#)
- [email-format-audit](#)
- [include-all-log-information](#)
- [no include-all-log-information](#)
- [health-check-email](#)
- [no health-check-email](#)
- [mail-server](#)
- [no mail-server](#)
- [mail-from](#)
- [no mail-from](#)
- [authentication-method](#)
- [pop3-server](#)
- [no pop3-server](#)
- [pop3-user-name](#)
- [no pop3-user-name](#)
- [pop3-password](#)
- [no pop3-password](#)
- [log-action test](#)
- [mail-server-advanced](#)
- [smtp-port](#)
- [connection-security-method](#)
- [no connection-security-method](#)
- [smtp-authentication](#)
- [no smtp-authentication](#)
- [user-name](#)
- [no user-name](#)
- [password](#)
- [no password](#)
- [ftp-log](#)
- [send-log-to-ftp](#)
- [no send-log-to-ftp](#)
- [server](#)
- [no server](#)
- [user-name](#)
- [no user-name](#)
- [password](#)
- [no password](#)
- [directory](#)
- [send-log](#)
- [file-format](#)
- [include-all-log-information](#)
- [no include-all-log-information](#)
- [solera](#)
- [solera-capture-stack-integration](#)
- [no solera-capture-stack-integration](#)
- [server](#)
- [no server](#)
- [protocol](#)
- [port](#)
- [user](#)
- [password](#)
- [deepsee-base-url](#)

- [pcap-base-url](#)
- [link-icon](#)
- [address-to-link](#)
- [method](#)
- [dns](#)
- [no dns](#)
- [log-action reset-name-cache](#)
- [log-action report-start](#)
- [log-action report-stop](#)
- [report-refresh](#)
- [log-action report-reset](#)
- [report-view](#)
- [show](#)
- [enable](#)
- [no enable](#)
- [enable](#)
- [no enable](#)
- [log aws](#)
- [enable](#)
- [no enable](#)
- [region](#)
- [group-name](#)
- [no group-name](#)
- [stream-name](#)
- [no stream-name](#)
- [synchronization-interval](#)
- [send-log-when-full](#)
- [no send-log-when-full](#)
- [export sdwan-conn-logs](#)
- [ecli/config-audit.cdl](#)
 - [log audit](#)
 - [enable](#)
 - [no enable](#)
 - [display-on-console](#)
 - [no display-on-console](#)
 - [supplemental-changes](#)
 - [no supplemental-changes](#)
 - [email audit](#)
 - [export audit](#)
- [ecli/log_show.cdl](#)
 - [show log](#)
- [ecli/voip.cdl](#)
 - [voip](#)
 - [flush-all](#)
 - [consistent-nat](#)
 - [no consistent-nat](#)
 - [sip](#)
 - [enable](#)
 - [no enable](#)
 - [h323](#)
 - [enable](#)
 - [no enable](#)
 - [access-rule-based](#)
 - [no access-rule-based](#)
 - [tcp](#)
 - [no tcp](#)
 - [transforms-in-service-object](#)
 - [no transforms-in-service-object](#)
 - [non-sip-packets](#)
 - [no non-sip-packets](#)
 - [b2bua-support](#)
 - [no b2bua-support](#)
 - [signaling-timeout](#)
 - [media-timeout](#)
 - [no signaling-port](#)
 - [signaling-port](#)
 - [endpoint-registration-anomaly-tracking](#)
 - [no endpoint-registration-anomaly-tracking](#)
 - [registration-tracking-interval](#)
 - [failed-registration-threshold](#)
 - [endpoint-block-interval](#)
 - [access-rule-based](#)
 - [no access-rule-based](#)
 - [only-gatekeeper-calls](#)
 - [no only-gatekeeper-calls](#)
 - [inactivity-timeout](#)
 - [no gatekeeper-ip](#)
 - [gatekeeper-ip](#)
- [ecli/voip_show.cdl](#)
 - [show voip](#)
- [ecli/wwan_show.cdl](#)
 - [show wwan](#)
- [ecli/security-services.cdl](#)
 - [security-services](#)
 - [synchronize](#)
 - [security](#)
 - [reduce-isdn-antivirus-traffic](#)

- [no reduce-isdn-antivirus-traffic](#)
- [drop-packets-at-reload](#)
- [no drop-packets-at-reload](#)
- [http-clientless-notification-timeout](#)
- [proxy-server](#)
- [enable](#)
- [no enable](#)
- [host](#)
- [no host](#)
- [port](#)
- [no port](#)
- [authentication](#)
- [no authentication](#)
- [portal](#)
- [no portal](#)
- [import signature](#)
- [ecli/dpi-ssh.cdl](#)
 - [dpi-ssh](#)
 - [enable](#)
 - [no enable](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [gateway](#)
 - [no gateway](#)
 - [application-firewall](#)
 - [no application-firewall](#)
 - [block-port-forwarding](#)
 - [no block-port-forwarding](#)
 - [include address](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [include service](#)
 - [exclude service](#)
 - [no exclude service](#)
 - [include user](#)
 - [exclude user](#)
 - [no exclude user](#)
- [ecli/content-filter.cdl](#)
 - [content-filter](#)
 - [filter-type](#)
 - [cfs](#)
 - [websense](#)
- [ecli/content-filter-cfs.cdl](#)
 - [max-url-caches](#)
 - [enable](#)
 - [no enable](#)
 - [block-if-server-unavailable](#)
 - [no block-if-server-unavailable](#)
 - [server-timeout](#)
 - [local-server](#)
 - [no local-server](#)
 - [exclude administrator](#)
 - [no exclude administrator](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [clear policies](#)
 - [clear policy](#)
 - [no policies](#)
 - [no policy](#)
 - [policy](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [source zone](#)
 - [destination zone](#)
 - [source address included](#)
 - [source address excluded](#)
 - [user included](#)
 - [user excluded](#)
 - [schedule](#)
 - [profile](#)
 - [action](#)
 - [enable](#)
 - [no enable](#)
 - [priority](#)
 - [no priority](#)
 - [import custom-category](#)
 - [custom-category](#)
 - [enable](#)
 - [no enable](#)
 - [no category-entries](#)
 - [no category-entry](#)
 - [category-entry](#)
 - [domain](#)
 - [no ratings](#)
 - [rating](#)
 - [no rating](#)
 - [synchronize local-server-info](#)
- [ecli/content-filter-objects.cdl](#)

- [no uri-list-objects](#)
- [no uri-list-groups](#)
- [no uri-list-object](#)
- [no uri-list-group](#)
- [uri-list-object](#)
- [uri-list-group](#)
- [name](#)
- [name](#)
- [type](#)
- [no entries](#)
- [no uri-list-group-members](#)
- [uri](#)
- [no uri](#)
- [no uris](#)
- [keyword](#)
- [no keyword](#)
- [no keywords](#)
- [domain](#)
- [no domain](#)
- [no domains](#)
- [location](#)
- [no location](#)
- [exclusion](#)
- [no exclusion](#)
- [auto-sync](#)
- [no auto-sync](#)
- [sync-interval](#)
- [no sync-interval](#)
- [export uris](#)
- [import uris](#)
- [export keywords](#)
- [import keywords](#)
- [uri-list-object](#)
- [no uri-list-object](#)
- [uri-list-group](#)
- [no uri-list-group](#)
- [no actions](#)
- [no action](#)
- [action](#)
- [name](#)
- [wipe-cookies](#)
- [no wipe-cookies](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [block page](#)
- [passphrase page](#)
- [passphrase password](#)
- [no passphrase password](#)
- [passphrase active-time](#)
- [confirm page](#)
- [confirm active-time](#)
- [bandwidth-management aggregation-method](#)
- [bandwidth-management egress](#)
- [no bandwidth-management egress](#)
- [bandwidth-management ingress](#)
- [no bandwidth-management ingress](#)
- [bandwidth-management usage-tracking](#)
- [no bandwidth-management usage-tracking](#)
- [no profiles](#)
- [no profile](#)
- [profile](#)
- [name](#)
- [uri-list allowed](#)
- [no uri-list allowed](#)
- [uri-list forbidden](#)
- [no uri-list forbidden](#)
- [uri-list search-order](#)
- [uri-list forbidden-operation](#)
- [category](#)
- [categories](#)
- [https-filtering](#)
- [no https-filtering](#)
- [smart-filter](#)
- [no smart-filter](#)
- [safe-search](#)
- [no safe-search](#)
- [threat-api](#)
- [no threat-api](#)
- [google-force-safe-search](#)
- [no google-force-safe-search](#)
- [youtube-restrict-mode](#)
- [no youtube-restrict-mode](#)
- [bing-force-safe-search](#)
- [no bing-force-safe-search](#)
- [consent required](#)
- [no consent required](#)
- [consent user-idle-timeout](#)
- [consent optional page-url](#)
- [no consent optional page-url](#)
- [consent mandatory page-url](#)
- [no consent mandatory page-url](#)
- [consent mandatory address](#)

- [no consent mandatory address](#)
- [custom-header insertion](#)
- [no custom-header insertion](#)
- [custom-header entry](#)
- [no custom-header entry](#)
- [no custom-header entries](#)
- [uuid](#)
- [no uuid](#)
- [uuid](#)
- [no uuid](#)
- [uuid](#)
- [no uuid](#)
- [uuid](#)
- [no uuid](#)
- [no uuid](#)
- [ecli/content-filter-websense.cdl](#)
 - [server](#)
 - [no server](#)
 - [port](#)
 - [user-name](#)
 - [no user-name](#)
 - [max-url-caches](#)
 - [https-content-filtering](#)
 - [no https-content-filtering](#)
 - [probe monitoring](#)
 - [no probe monitoring](#)
 - [probe interval](#)
 - [probe deactivate-after](#)
 - [probe reactivate-after](#)
 - [block-if-server-unavailable](#)
 - [no block-if-server-unavailable](#)
 - [server-timeout](#)
 - [block activex](#)
 - [no block activex](#)
 - [block java](#)
 - [no block java](#)
 - [block flash](#)
 - [no block flash](#)
 - [block cookies](#)
 - [no block cookies](#)
 - [block http-proxy-access](#)
 - [no block http-proxy-access](#)
 - [exclude web-features-domains](#)
 - [no exclude web-features-domains](#)
 - [exclude administrator](#)
 - [no exclude administrator](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [blocking-page](#)
- [ecli/client-enforcement-enhancement.cdl](#)
 - [endpoint-security](#)
 - [enable](#)
 - [no enable](#)
 - [alert-message enable](#)
 - [no alert-message enable](#)
 - [log cfs](#)
 - [no log cfs](#)
 - [log ips](#)
 - [no log ips](#)
 - [log appctrl](#)
 - [no log appctrl](#)
 - [log botnet-geoip](#)
 - [no log botnet-geoip](#)
 - [log gav-gas-atp](#)
 - [no log gav-gas-atp](#)
 - [user-sso enable](#)
 - [no user-sso enable](#)
- [ecli/client-enforcement-enhancement-objects.cdl](#)
 - [no profiles](#)
 - [no profile](#)
 - [profile](#)
 - [name](#)
 - [grace-period](#)
 - [no grace-period](#)
 - [bypass-guest-ce](#)
 - [no bypass-guest-ce](#)
 - [service-capture-client](#)
 - [no service-capture-client](#)
 - [no policies](#)
 - [no policy](#)
 - [policy](#)
 - [name](#)
 - [source zone](#)
 - [source address included](#)
 - [source address excluded](#)
 - [profile](#)
 - [enable](#)
 - [no enable](#)
 - [priority](#)
 - [no priority](#)

- `ecli/anti-spam.cdl`
 - [`anti-spam`](#)
 - [`start anti-spam-capture`](#)
 - [`stop anti-spam-capture`](#)
 - [`clear anti-spam-capture`](#)
 - [`export capture`](#)
 - [`grid-ip-check`](#)
 - [`enable`](#)
 - [`destination-mail-server public`](#)
 - [`no enable`](#)
 - [`action likely-spam`](#)
 - [`action definite-spam`](#)
 - [`action likely-phishing`](#)
 - [`action definite-phishing`](#)
 - [`action likely-virus`](#)
 - [`action definite-virus`](#)
 - [`allow-list`](#)
 - [`no allow-list`](#)
 - [`reject-list`](#)
 - [`no reject-list`](#)
 - [`service-down`](#)
 - [`junk-box down`](#)
 - [`junk-box secure-http`](#)
 - [`no junk-box secure-http`](#)
 - [`junk-box port`](#)
 - [`no junk-box port`](#)
 - [`probe interval`](#)
 - [`probe timeout`](#)
 - [`success-threshold`](#)
 - [`failure-threshold`](#)
 - [`mail-server`](#)
 - [`no mail-server`](#)
 - [`junk-store-username`](#)
 - [`junk-store-password`](#)
 - [`destination-mail-address-as-junk-store`](#)
 - [`no destination-mail-address-as-junk-store`](#)
 - [`junk-store-ip`](#)
 - [`no junk-store-ip`](#)
 - [`system-detection`](#)
 - [`no system-detection`](#)
- `ecli/ips.cdl`
 - [`intrusion-prevention`](#)
 - [`update-signatures`](#)
 - [`enable`](#)
 - [`no enable`](#)
 - [`signature-group high-priority`](#)
 - [`signature-group medium-priority`](#)
 - [`signature-group low-priority`](#)
 - [`no signature-group high-priority`](#)
 - [`no signature-group medium-priority`](#)
 - [`no signature-group low-priority`](#)
 - [`reset`](#)
 - [`category`](#)
 - [`exclusion`](#)
 - [`from`](#)
 - [`to`](#)
 - [`no exclusion`](#)
 - [`name`](#)
 - [`id`](#)
 - [`prevention`](#)
 - [`no prevention`](#)
 - [`detection`](#)
 - [`no detection`](#)
 - [`included users`](#)
 - [`excluded users`](#)
 - [`included ip`](#)
 - [`excluded ip`](#)
 - [`no excluded`](#)
 - [`schedule`](#)
 - [`log-redundancy`](#)
 - [`no log-redundancy`](#)
 - [`category`](#)
 - [`prevention`](#)
 - [`no prevention`](#)
 - [`detection`](#)
 - [`no detection`](#)
 - [`included users`](#)
 - [`excluded users`](#)
 - [`included ip`](#)
 - [`excluded ip`](#)
 - [`no excluded`](#)
 - [`schedule`](#)
 - [`log-redundancy`](#)
 - [`no log-redundancy`](#)
 - [`priority`](#)
 - [`direction`](#)
 - [`no direction`](#)
- `ecli/gav.cdl`
 - [`gateway-antivirus`](#)
 - [`update-signatures`](#)

- [enable](#)
- [no enable](#)
- [signature](#)
- [no signature](#)
- [inbound-inspection](#)
- [no inbound-inspection](#)
- [outbound-inspection](#)
- [no outbound-inspection](#)
- [restrict password-protected-zip](#)
- [no restrict password-protected-zip](#)
- [restrict ms-office-macros](#)
- [no restrict ms-office-macros](#)
- [restrict packed-executables](#)
- [no restrict packed-executables](#)
- [exclusion-object http](#)
- [exclusion-object ftp](#)
- [exclusion-object imap](#)
- [exclusion-object smtp](#)
- [exclusion-object pop3](#)
- [exclusion-object cifs-netbios](#)
- [no exclusion-object](#)
- [reset-settings](#)
- [cloud anti-virus-database](#)
- [no cloud anti-virus-database](#)
- [cloud exclusion](#)
- [no cloud exclusion](#)
- [no cloud exclusions](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [eicar-detection](#)
- [no eicar-detection](#)
- [http-byte-range](#)
- [no http-byte-range](#)
- [ftp-rest](#)
- [no ftp-rest](#)
- [scan-high-compression](#)
- [no scan-high-compression](#)
- [block-multiple-compress-files](#)
- [no block-multiple-compress-files](#)
- [detection-only](#)
- [no detection-only](#)
- [http-clientless-notification](#)
- [no http-clientless-notification](#)
- [no notification-message](#)
- [notification-message](#)
- [exclusion](#)
- [from](#)
- [to](#)
- [no exclusion](#)
- [ecli/capture-atp.cdl](#)
 - [capture-atp](#)
 - [enable](#)
 - [no enable](#)
 - [location](#)
 - [local-name-or-ip](#)
 - [no local-name-or-ip](#)
 - [file-type](#)
 - [no file-type](#)
 - [file-size](#)
 - [exclude address for-capture-atp](#)
 - [no exclude address for-capture-atp](#)
 - [exclude md5-entry](#)
 - [no exclude md5-entry](#)
 - [no exclude md5-entries](#)
 - [exclude http-entry](#)
 - [no exclude http-entry](#)
 - [no exclude http-entries](#)
 - [await-verdict](#)
 - [exclude address for-block-until-verdict](#)
 - [no exclude address for-block-until-verdict](#)
 - [exclude file-type](#)
 - [no exclude file-type](#)
 - [test uftp-connectivity](#)
 - [clear uftp-connectivity](#)
 - [refresh uftp-connectivity](#)
 - [check md5-query-status](#)
 - [clear md5-query-status](#)
 - [refresh md5-query-status](#)
- [ecli/match-object.cdl](#)
 - [no match-object](#)
 - [no match-objects](#)
 - [match-object](#)
 - [no type](#)
 - [type](#)
 - [name](#)
 - [match-type](#)
 - [no match-type](#)
 - [enable](#)
 - [no enable](#)
 - [offset](#)

- [depth](#)
- [min-size](#)
- [max-size](#)
- [negative-matching](#)
- [no negative-matching](#)
- [no input-representation](#)
- [input-representation](#)
- [content-entry](#)
- [no content-entry](#)
- [no content-entries](#)
- [pre-defined-regex](#)
- [no pre-defined-regex](#)
- [browser](#)
- [no browser](#)
- [no browsers](#)
- [custom-header](#)
- [no custom-header](#)
- [email-size](#)
- [no email-size](#)
- [ftp-command](#)
- [no ftp-command](#)
- [no ftp-commands](#)
- [argument](#)
- [no argument](#)
- [no arguments](#)
- [ips category](#)
- [no ips category](#)
- [no ips categories](#)
- [ips policy](#)
- [no ips policy](#)
- [no ips policies](#)
- [category](#)
- [no category](#)
- [no categories](#)
- [application](#)
- [no application](#)
- [no applications](#)
- [signature](#)
- [no signature](#)
- [no signatures](#)
- [ecli/action-object.cdl](#)
 - [action-object](#)
 - [no action-object](#)
 - [no action-objects](#)
 - [name](#)
 - [action](#)
 - [no content](#)
 - [content](#)
 - [no color](#)
 - [color](#)
 - [bandwidth-management](#)
 - [aggregation-method](#)
 - [no egress](#)
 - [egress bandwidth-object](#)
 - [no ingress](#)
 - [ingress bandwidth-object](#)
 - [usage-tracking](#)
 - [no usage-tracking](#)
- [ecli/email-object.cdl](#)
 - [no email-object](#)
 - [no email-objects](#)
 - [email-object](#)
 - [name](#)
 - [no match-type](#)
 - [match-type](#)
 - [content-entry](#)
 - [no content-entry](#)
 - [no content-entries](#)
- [ecli/app-rules.cdl](#)
 - [app-rules](#)
 - [enable](#)
 - [no enable](#)
 - [log-redundancy](#)
 - [no log-redundancy](#)
 - [no policy](#)
 - [no policies](#)
 - [policy](#)
 - [name](#)
 - [type](#)
 - [source address](#)
 - [destination address](#)
 - [address](#)
 - [exclusion address](#)
 - [no exclusion address](#)
 - [source service](#)
 - [destination service](#)
 - [match-object](#)
 - [action-object](#)
 - [users](#)

- [no users](#)
- [mail-from included](#)
- [mail-from excluded](#)
- [no mail-from](#)
- [rcpt-to included](#)
- [rcpt-to excluded](#)
- [no rcpt-to](#)
- [schedule](#)
- [enable](#)
- [no enable](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [logging](#)
- [no logging](#)
- [log individual](#)
- [no log individual](#)
- [ips-message-format](#)
- [no ips-message-format](#)
- [app-control-message-format](#)
- [no app-control-message-format](#)
- [cfs-message-format](#)
- [no cfs-message-format](#)
- [log redundancy](#)
- [no log redundancy](#)
- [connection-side](#)
- [direction](#)
- [zone](#)
- [cfs-list allow](#)
- [no cfs-list allow](#)
- [cfs-list forbidden](#)
- [no cfs-list forbidden](#)
- [safe-search](#)
- [no safe-search](#)
- [youtube-for-schools](#)
- [no youtube-for-schools](#)
- [school-id](#)
- [no school-id](#)
- [ecli/app-control.cdl](#)
 - [app-control](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [log-all](#)
 - [no log-all](#)
 - [log-filename](#)
 - [no log-filename](#)
 - [log-redundancy filter](#)
 - [no log-redundancy filter](#)
 - [reset](#)
 - [category](#)
 - [exclusion list](#)
 - [no exclusion list](#)
 - [name](#)
 - [id](#)
 - [block](#)
 - [no block](#)
 - [log](#)
 - [no log](#)
 - [included users](#)
 - [excluded users](#)
 - [included ip](#)
 - [excluded ip](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
 - [no log-redundancy](#)
 - [block](#)
 - [no block](#)
 - [log](#)
 - [no log](#)
 - [included users](#)
 - [excluded users](#)
 - [included ip](#)
 - [excluded ip](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)
 - [no log-redundancy](#)
 - [category](#)
 - [application](#)
 - [block](#)
 - [no block](#)
 - [log](#)
 - [no log](#)
 - [included users](#)
 - [excluded users](#)
 - [included ip](#)
 - [excluded ip](#)
 - [no excluded](#)
 - [schedule](#)
 - [log-redundancy](#)

- [no log-redundancy](#)
- [ecli/rbl.cdl](#)
 - [rbl](#)
 - [enable](#)
 - [no enable](#)
 - [dns](#)
 - [no dns](#)
 - [service](#)
 - [no service](#)
 - [no services](#)
 - [clear statistics](#)
 - [blacklist](#)
 - [no blacklist](#)
 - [whitelist](#)
 - [no whitelist](#)
 - [enable](#)
 - [no enable](#)
 - [domain](#)
 - [blocked-responses](#)
 - [no blocked-responses](#)
- [ecli/dpi-ssl.cdl](#)
 - [dpi-ssl](#)
 - [export dpi-ssl-client certificate](#)
 - [import exclusions](#)
 - [enable](#)
 - [no enable](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [gateway](#)
 - [no gateway](#)
 - [application-firewall](#)
 - [no application-firewall](#)
 - [content-filter](#)
 - [no content-filter](#)
 - [authenticate-server-for-decrypted-connections](#)
 - [no authenticate-server-for-decrypted-connections](#)
 - [expired-ca](#)
 - [no expired-ca](#)
 - [deployment-server-domains](#)
 - [no deployment-server-domains](#)
 - [bypass-decryption](#)
 - [no bypass-decryption](#)
 - [audit-built-in-exclusion](#)
 - [no audit-built-in-exclusion](#)
 - [authenticate-server](#)
 - [no authenticate-server](#)
 - [open-failed-connections](#)
 - [no open-failed-connections](#)
 - [resigning-authority](#)
 - [include address](#)
 - [exclude address](#)
 - [no exclude address](#)
 - [include service](#)
 - [exclude service](#)
 - [no exclude service](#)
 - [include user](#)
 - [exclude user](#)
 - [no exclude user](#)
 - [clear connection-failures](#)
 - [reject](#)
 - [accept](#)
 - [no common-name](#)
 - [no common-names](#)
 - [common-name](#)
 - [cfs-categories](#)
 - [no cfs-categories](#)
 - [exclude cfs-category-unavailable](#)
 - [no exclude cfs-category-unavailable](#)
 - [enable](#)
 - [no enable](#)
 - [intrusion-prevention](#)
 - [no intrusion-prevention](#)
 - [gateway](#)
 - [no gateway](#)
 - [application-firewall](#)
 - [no application-firewall](#)
 - [include address](#)
 - [exclude address](#)
 - [include user](#)
 - [exclude user](#)
 - [no exclude](#)
 - [ssl-server](#)
 - [no ssl-server](#)
 - [no ssl-servers](#)
- [ecli/geo-ip.cdl](#)
 - [geo-ip](#)
 - [custom-list](#)
 - [enable](#)
 - [no enable](#)

- [override-countries](#)
- [no override-countries](#)
- [address](#)
- [no address](#)
- [no addresses](#)
- [country](#)
- [comment](#)
- [no comment](#)
- [block connections](#)
- [no block connections](#)
- [block database-not-downloaded](#)
- [no block database-not-downloaded](#)
- [logging](#)
- [no logging](#)
- [block country](#)
- [no block country](#)
- [block countries](#)
- [no block countries](#)
- [no exclude](#)
- [exclude](#)
- [include block-details](#)
- [no include block-details](#)
- [alert-text](#)
- [no alert-text](#)
- [logo-icon](#)
- [default blocked-page](#)
- [ecli/botnet.cdl](#)
 - [botnet](#)
 - [custom-list](#)
 - [dynamic-list](#)
 - [block connections](#)
 - [no block connections](#)
 - [block database-not-downloaded](#)
 - [no block database-not-downloaded](#)
 - [enable](#)
 - [no enable](#)
 - [address](#)
 - [no address](#)
 - [no addresses](#)
 - [name](#)
 - [group](#)
 - [enable](#)
 - [no enable](#)
 - [comment](#)
 - [no comment](#)
 - [enable](#)
 - [no enable](#)
 - [botnet-flush](#)
 - [botnet-download](#)
 - [periodical-download](#)
 - [no periodical-download](#)
 - [download-interval](#)
 - [protocol](#)
 - [ftp server-ip-address](#)
 - [no ftp server-ip-address](#)
 - [ftp login](#)
 - [no ftp login](#)
 - [ftp password](#)
 - [no ftp password](#)
 - [https login](#)
 - [no https login](#)
 - [https password](#)
 - [no https password](#)
 - [ftp directory-path](#)
 - [no ftp directory-path](#)
 - [ftp file-name](#)
 - [no ftp file-name](#)
 - [https url-name](#)
 - [no https url-name](#)
 - [logging](#)
 - [no logging](#)
 - [exclude](#)
 - [no exclude](#)
 - [include block-details](#)
 - [no include block-details](#)
 - [alert-text](#)
 - [no alert-text](#)
 - [logo-icon](#)
 - [default blocked-page](#)
- [ecli/anti-spyware.cdl](#)
 - [anti-spyware](#)
 - [update-signatures](#)
 - [enable](#)
 - [no enable](#)
 - [signature-group](#)
 - [no signature-group](#)
 - [reset](#)
 - [inspection inbound](#)
 - [no inspection inbound](#)
 - [inspection outbound](#)

- [no inspection outbound](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [http-clientless-notification](#)
- [no http-clientless-notification](#)
- [message](#)
- [no message](#)
- [exclusion](#)
- [from](#)
- [to](#)
- [no exclusion list](#)
- [no exclusion entry](#)
- [no exclusion entries](#)
- [product](#)
- [name](#)
- [id](#)
- [prevention](#)
- [no prevention](#)
- [detection](#)
- [no detection](#)
- [included](#)
- [excluded](#)
- [no excluded](#)
- [schedule](#)
- [log-redundancy](#)
- [no log-redundancy](#)
- [product](#)
- [danger-level](#)
- [prevention](#)
- [no prevention](#)
- [detection](#)
- [no detection](#)
- [included](#)
- [excluded](#)
- [no excluded](#)
- [schedule](#)
- [log-redundancy](#)
- [no log-redundancy](#)
- [ecli/security-services_show.cdl](#)
 - [show security-services](#)
- [ecli/dpi-ssh_show.cdl](#)
 - [show dpi-ssh](#)
- [ecli/content-filter_show.cdl](#)
 - [show content-filter](#)
- [ecli/client-enforcement-enhancement_show.cdl](#)
 - [show endpoint-security](#)
- [ecli/anti-spam_show.cdl](#)
 - [show anti-spam](#)
- [ecli/ips_show.cdl](#)
 - [show intrusion-prevention](#)
- [ecli/gav_show.cdl](#)
 - [show gateway-antivirus](#)
- [ecli/capture-atp_show.cdl](#)
 - [show capture-atp](#)
- [ecli/match-object_show.cdl](#)
 - [show match-objects](#)
 - [show match-object](#)
- [ecli/action-object_show.cdl](#)
 - [show action-objects](#)
 - [show action-object](#)
- [ecli/email-object_show.cdl](#)
 - [show email-objects](#)
 - [show email-object](#)
- [ecli/app-rules_show.cdl](#)
 - [show app-rules](#)
- [ecli/app-control_show.cdl](#)
 - [show app-control](#)
- [ecli/rbl_show.cdl](#)
 - [show rbl](#)
- [ecli/dpi-ssl_show.cdl](#)
 - [show dpi-ssl](#)
- [ecli/geo-ip_show.cdl](#)
 - [show geo-ip](#)
- [ecli/botnet_show.cdl](#)
 - [show botnet](#)
- [ecli/anti-spyware_show.cdl](#)

- [show anti-spyware](#)
- [ecli/vpn.cdl](#)
 - [vpn](#)
 - [no vpn policy](#)
 - [no vpn policies](#)
 - [no vpn policies-ipv4](#)
 - [no vpn policies-ipv6](#)
 - [renegotiate tunnel](#)
 - [enable](#)
 - [no enable](#)
 - [firewall-identifier](#)
 - [ike-dpd](#)
 - [enable](#)
 - [no enable](#)
 - [interval](#)
 - [trigger](#)
 - [idle-dpd](#)
 - [no idle-dpd](#)
 - [idle-dpd-interval](#)
 - [frag-packets](#)
 - [enable](#)
 - [no enable](#)
 - [ignore-df-bit](#)
 - [no ignore-df-bit](#)
 - [nat-traversal](#)
 - [no nat-traversal](#)
 - [cleanup-tunnels](#)
 - [no cleanup-tunnels](#)
 - [preserve-ike-port](#)
 - [no preserve-ike-port](#)
 - [ocsp-checking](#)
 - [no ocsp-checking](#)
 - [responder-url](#)
 - [no responder-url](#)
 - [traps-on-change](#)
 - [no traps-on-change](#)
 - [use-radius](#)
 - [no use-radius](#)
 - [dns server](#)
 - [no dns server](#)
 - [wins](#)
 - [no wins](#)
 - [ikev2](#)
 - [send-cookie](#)
 - [no send-cookie](#)
 - [send-invalid-spi](#)
 - [no send-invalid-spi](#)
 - [proposal dh-group](#)
 - [proposal encryption](#)
 - [proposal authentication](#)
 - [policy](#)
 - [no policy](#)
 - [no policies](#)
 - [name](#)
 - [name](#)
 - [enable](#)
 - [no enable](#)
 - [gateway primary](#)
 - [no gateway primary](#)
 - [gateway secondary](#)
 - [no gateway secondary](#)
 - [auth-method](#)
 - [auth-method](#)
 - [export group-vpn](#)
 - [auth-method](#)
 - [ap-client-id](#)
 - [no ap-client-id](#)
 - [use-default-key](#)
 - [no use-default-key](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [shared-secret](#)
 - [no shared-secret](#)
 - [ike-id local](#)
 - [no ike-id local](#)
 - [ike-id peer](#)
 - [no ike-id peer](#)
 - [certificate](#)
 - [no certificate](#)
 - [ike-id local](#)
 - [ike-id peer](#)
 - [no ike-id peer](#)
 - [client-id peer](#)
 - [no client-id peer](#)
 - [peer id](#)
 - [peer match-issuer](#)
 - [no peer match-issuer](#)
 - [user-name](#)
 - [no user-name](#)
 - [user-password](#)
 - [no user-password](#)

- [network local](#)
- [no network local](#)
- [network remote](#)
- [no network remote](#)
- [network local](#)
- [no network local](#)
- [network remote](#)
- [no network remote](#)
- [proposal ike](#)
- [proposal ipsec](#)
- [no proposal ipsec](#)
- [client cache-xauth](#)
- [client virtual-adaptor](#)
- [client allow-connections-to](#)
- [client default-route](#)
- [no client default-route](#)
- [client access-list](#)
- [no client access-list](#)
- [client simple-provisioning](#)
- [no client simple-provisioning](#)
- [keep-alive](#)
- [no keep-alive](#)
- [suppress-auto-add-rule](#)
- [no suppress-auto-add-rule](#)
- [require-xauth](#)
- [no require-xauth](#)
- [anti-replay](#)
- [no anti-replay](#)
- [advanced-routing](#)
- [no advanced-routing](#)
- [transport-mode](#)
- [no transport-mode](#)
- [netbios](#)
- [no netbios](#)
- [multicast](#)
- [no multicast](#)
- [permit-acceleration](#)
- [no permit-acceleration](#)
- [wxa-group](#)
- [no wxa-group](#)
- [no translated-network](#)
- [translated-network](#)
- [apply-nat](#)
- [no apply-nat](#)
- [no ocsip-checking](#)
- [ocsip-checking](#)
- [responder-url](#)
- [no responder-url](#)
- [management](#)
- [no management](#)
- [user-login](#)
- [no user-login](#)
- [default-lan-gateway](#)
- [no default-lan-gateway](#)
- [bound-to](#)
- [local-ip](#)
- [preempt-secondary-gateway](#)
- [no preempt-secondary-gateway](#)
- [client-authentication](#)
- [suppress-trigger-packet](#)
- [no suppress-trigger-packet](#)
- [accept-hash](#)
- [no accept-hash](#)
- [send-hash](#)
- [no send-hash](#)
- [accept-multiple-proposals](#)
- [no accept-multiple-proposals](#)
- [ike-mode-configuration](#)
- [no ike-mode-configuration](#)
- [allow-sonicpointn-layer3](#)
- [no allow-sonicpointn-layer3](#)
- [ecli/l2tp-server.cdl](#)
 - [l2tp-server](#)
 - [enable](#)
 - [no enable](#)
 - [keep-alive](#)
 - [dns](#)
 - [no dns](#)
 - [wins](#)
 - [no wins](#)
 - [ip-pool](#)
 - [no user-group](#)
 - [user-group](#)
 - [ppp.protocol](#)
 - [no ppp.protocol](#)
 - [no ppp.protocols](#)
 - [disconnect session](#)
- [ecli/dhcp-over-vpn.cdl](#)
 - [dhcp-over-vpn](#)
 - [clear lease](#)

- [clear leases](#)
- [mode](#)
- [central](#)
- [remote](#)
- [internal-dhcp](#)
- [no internal-dhcp](#)
- [global-vpn](#)
- [no global-vpn](#)
- [remote](#)
- [no remote](#)
- [send-requests](#)
- [no send-requests](#)
- [dhcp-server](#)
- [no dhcp-server](#)
- [no dhcp-servers](#)
- [ip](#)
- [no relay-ip](#)
- [relay-ip](#)
- [bound-to](#)
- [accept-bridged-wlan-request](#)
- [no accept-bridged-wlan-request](#)
- [no relay-ip](#)
- [relay-ip](#)
- [no management-ip](#)
- [management-ip](#)
- [block-spoof](#)
- [no block-spoof](#)
- [temp-lease](#)
- [no temp-lease](#)
- [lease-time](#)
- [static-device](#)
- [no static-device](#)
- [no static-devices](#)
- [ip](#)
- [mac](#)
- [excluded-device](#)
- [no excluded-device](#)
- [no excluded-devices](#)
- [mac](#)
- [clear dhcp-servers](#)
- [clear static-devices](#)
- [clear excluded-lan-devices](#)
- [ecli/vpn_show.cdl](#)
 - [show vpn](#)
- [ecli/ssl-vpn.cdl](#)
 - [ssl-vpn server](#)
 - [logout](#)
 - [access](#)
 - [no access](#)
 - [port](#)
 - [certificate](#)
 - [use-radius](#)
 - [no use-radius](#)
 - [user-domain](#)
 - [no user-domain](#)
 - [management web](#)
 - [no management web](#)
 - [management ssh](#)
 - [no management ssh](#)
 - [session-timeout](#)
 - [inactivity-check](#)
 - [no inactivity-check](#)
 - [download-url](#)
 - [ssl-vpn portal](#)
 - [site-title](#)
 - [banner-title](#)
 - [home-page-message](#)
 - [login-message](#)
 - [auto-launch](#)
 - [no auto-launch](#)
 - [cache-control](#)
 - [no cache-control](#)
 - [display-link](#)
 - [no display-link](#)
 - [logo](#)
 - [ssl-vpn epc-profile](#)
 - [ssl-vpn profile](#)
 - [enable-epc](#)
 - [no enable-epc](#)
 - [fallback-options](#)
 - [device-profile](#)
 - [device-profile](#)
 - [no device-profile](#)
 - [no device-profiles](#)
 - [name](#)
 - [description](#)
 - [no description](#)
 - [enable](#)
 - [no enable](#)
 - [action](#)

- [network-address](#)
- [no network-address](#)
- [deny-message](#)
- [no deny-message](#)
- [quarantine-message](#)
- [no quarantine-message](#)
- [wlan-tunnel-interface](#)
- [no wlan-tunnel-interface](#)
- [security](#)
- [routes](#)
- [client](#)
- [no all-attributes](#)
- [type](#)
- [no type](#)
- [firewall](#)
- [no firewall](#)
- [certification](#)
- [no certification](#)
- [application](#)
- [no application](#)
- [directory](#)
- [no directory](#)
- [equipment](#)
- [no equipment](#)
- [domain](#)
- [no domain](#)
- [file](#)
- [no file](#)
- [registry](#)
- [no registry](#)
- [os-version](#)
- [no os-version](#)
- [dns inherit](#)
- [dns primary](#)
- [no dns primary](#)
- [dns secondary](#)
- [no dns secondary](#)
- [dns search-list](#)
- [no dns search-list](#)
- [no dns search-lists](#)
- [wins primary](#)
- [no wins primary](#)
- [wins secondary](#)
- [no wins secondary](#)
- [auto-update](#)
- [no auto-update](#)
- [exit-after-disconnect](#)
- [no exit-after-disconnect](#)
- [netbios-over-sslvpn](#)
- [no netbios-over-sslvpn](#)
- [touch-id-authentication](#)
- [no touch-id-authentication](#)
- [fingerprint-authentication](#)
- [no fingerprint-authentication](#)
- [uninstall-after-exit](#)
- [no uninstall-after-exit](#)
- [create-connection-profile](#)
- [no create-connection-profile](#)
- [cache](#)
- [no cache](#)
- [tunnel-all](#)
- [no tunnel-all](#)
- [route](#)
- [no route](#)
- [no routes](#)
- [ssl-vpn virtual-office](#)
- [ssl-vpn logout](#)
- [bookmark](#)
- [no bookmark](#)
- [no bookmarks](#)
- [name](#)
- [host](#)
- [no host](#)
- [service](#)
- [screen-size](#)
- [colors](#)
- [application-path](#)
- [no application-path](#)
- [start-in-folder](#)
- [no start-in-folder](#)
- [automatic-login](#)
- [no automatic-login](#)
- [redirect-clipboard](#)
- [no redirect-clipboard](#)
- [redirect-audio](#)
- [no redirect-audio](#)
- [auto-reconnection](#)
- [no auto-reconnection](#)
- [desktop-background](#)
- [no desktop-background](#)
- [window-drag](#)
- [no window-drag](#)

- [animation](#)
 - [no animation](#)
 - [view-only](#)
 - [no view-only](#)
 - [share-desktop](#)
 - [no share-desktop](#)
 - [automatic-accept-host-key](#)
 - [no automatic-accept-host-key](#)
 - [display-on-mobile](#)
 - [no display-on-mobile](#)
- `ecli/ssl-vpn_show.cdl`
 - [show ssl-vpn](#)
- `ecli/ha.cdl`
 - [high-availability](#)
 - [heartbeat-interval](#)
 - [failover-trigger-level](#)
 - [probe interval](#)
 - [probe count](#)
 - [election-delay-time](#)
 - [route-hold-down-time](#)
 - [no route-hold-down-time](#)
 - [sdwan-hold-down-time](#)
 - [failover-when-aggregate-down](#)
 - [no failover-when-aggregate-down](#)
 - [include-certificates-keys](#)
 - [no include-certificates-keys](#)
 - [synchronize settings](#)
 - [synchronize firmware](#)
 - [force-failover](#)
 - [no mode](#)
 - [mode](#)
 - [primary-serial](#)
 - [secondary-serial](#)
 - [no secondary-serial](#)
 - [stateful-synchronization](#)
 - [no stateful-synchronization](#)
 - [dpi-interface](#)
 - [no dpi-interface](#)
 - [control-interface](#)
 - [no control-interface](#)
 - [data-interface](#)
 - [no data-interface](#)
 - [preempt](#)
 - [no preempt](#)
 - [encryption](#)
 - [no encryption](#)
 - [virtual-mac](#)
 - [no virtual-mac](#)
 - [monitoring](#)
 - [monitoring interface](#)
 - [link-monitoring](#)
 - [no link-monitoring](#)
 - [no primary](#)
 - [primary](#)
 - [no secondary](#)
 - [secondary](#)
 - [allow-management](#)
 - [no allow-management](#)
 - [logical-probe](#)
 - [no logical-probe](#)
 - [override-virtual-mac](#)
 - [no override-virtual-mac](#)
- `ecli/ha_show.cdl`
 - [show high-availability](#)
- `ecli/sdwan-perf-class-obj.cdl`
 - [sla-class-object](#)
 - [no sla-class-object](#)
 - [no sla-class-objects](#)
 - [name](#)
 - [include](#)
 - [no include](#)
 - [latency](#)
 - [no latency](#)
 - [jitter](#)
 - [no jitter](#)
 - [packet-loss](#)
 - [no packet-loss](#)
 - [comment](#)
 - [no comment](#)
- `ecli/sdwan-probe.cdl`
 - [sla-probe](#)
 - [no sla-probe](#)
 - [no sla-probes](#)
 - [name](#)
 - [sdwan-group](#)
 - [no probe target](#)
 - [probe target](#)
 - [probe type](#)

- [probe interval](#)
- [reply-timeout](#)
- [interval missed](#)
- [interval successful](#)
- [rst-as-miss](#)
- [no rst-as-miss](#)
- [comment](#)
- [no comment](#)
- ecli/sdwan-group.cdl
 - [sdwan](#)
 - [no group](#)
 - [no groups](#)
 - [group](#)
 - [name](#)
 - [interface](#)
 - [no interface](#)
 - [no interfaces](#)
 - [priority](#)
- ecli/sdwan-path-selection-profile.cdl
 - [path-selection-profile](#)
 - [no path-selection-profile](#)
 - [no path-selection-profiles](#)
 - [name](#)
 - [sdwan-group](#)
 - [no sdwan-group](#)
 - [sla-probe](#)
 - [no sla-probe](#)
 - [sla-class](#)
 - [no sla-class](#)
 - [backup-interface](#)
 - [no backup-interface](#)
 - [probe-default-up](#)
 - [no probe-default-up](#)
 - [reset-connections](#)
 - [no reset-connections](#)
- ecli/sdwan-perf-class-obj_show.cdl
 - [show sdwan sla-class-objects](#)
 - [show sdwan sla-class-object](#)
- ecli/sdwan-probe_show.cdl
 - [show sdwan sla-probes](#)
 - [show sdwan sla-probe](#)
- ecli/sdwan-group_show.cdl
 - [show sdwan group](#)
 - [show sdwan groups](#)
- ecli/sdwan-path-selection-profile_show.cdl
 - [show sdwan path-selection-profiles](#)
 - [show sdwan path-selection-profile](#)
- ecli/security-action-profile.cdl
 - [no security-action-profile](#)
 - [no security-action-profiles](#)
 - [security-action-profile](#)
 - [clone security-action-profile](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [bandwidth-management](#)
 - [aggregation-method](#)
 - [egress enable](#)
 - [no egress enable](#)
 - [egress bandwidth-object](#)
 - [no egress bandwidth-object](#)
 - [ingress enable](#)
 - [no ingress enable](#)
 - [ingress bandwidth-object](#)
 - [no ingress bandwidth-object](#)
 - [usage-tracking](#)
 - [no usage-tracking](#)
 - [quality-of-service class-of-service](#)
 - [cos-override](#)
 - [no cos-override](#)
 - [no quality-of-service](#)
 - [quality-of-service dscp](#)
 - [gateway-antivirus](#)
 - [enable](#)
 - [no enable](#)
 - [cloud](#)
 - [no cloud](#)
 - [inbound](#)
 - [no inbound](#)
 - [outbound](#)
 - [no outbound](#)
 - [prevent](#)
 - [no prevent](#)
 - [packet-monitor](#)
 - [no packet-monitor](#)

- [log](#)
- [no log](#)
- [password-protected-zip](#)
- [no password-protected-zip](#)
- [ms-office-macros](#)
- [no ms-office-macros](#)
- [packed-executables](#)
- [no packed-executables](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [eicar-detection](#)
- [no eicar-detection](#)
- [http-byte-range](#)
- [no http-byte-range](#)
- [ftp-rest](#)
- [no ftp-rest](#)
- [scan-high-compression](#)
- [no scan-high-compression](#)
- [threat](#)
- [enable](#)
- [no enable](#)
- [based-on](#)
- [prevent enable](#)
- [no prevent enable](#)
- [prevent profile](#)
- [packet-monitor enable](#)
- [no packet-monitor enable](#)
- [packet-monitor profile](#)
- [log enable](#)
- [no log enable](#)
- [log profile](#)
- [log redundancy](#)
- [no log redundancy](#)
- [signature-group high-priority](#)
- [signature-group medium-priority](#)
- [signature-group low-priority](#)
- [no signature-group high-priority](#)
- [no signature-group medium-priority](#)
- [no signature-group low-priority](#)
- [anti-spyware](#)
- [enable](#)
- [no enable](#)
- [inbound](#)
- [no inbound](#)
- [outbound](#)
- [no outbound](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [http-clientless-notification](#)
- [no http-clientless-notification](#)
- [signature-group high-priority](#)
- [signature-group medium-priority](#)
- [signature-group low-priority](#)
- [no signature-group high-priority](#)
- [no signature-group medium-priority](#)
- [no signature-group low-priority](#)
- [botnet](#)
- [enable](#)
- [no enable](#)
- [packet-monitor](#)
- [no packet-monitor](#)
- [log enable](#)
- [no log enable](#)
- [log redundancy](#)
- [no log redundancy](#)
- [content-filter](#)
- [enable](#)
- [no enable](#)
- [action](#)
- [safe-search](#)
- [no safe-search](#)
- [google-force-safe-search](#)
- [no google-force-safe-search](#)
- [youtube-restrict-mode](#)
- [no youtube-restrict-mode](#)
- [bing-force-safe-search](#)
- [no bing-force-safe-search](#)
- [wipe-cookies](#)
- [no wipe-cookies](#)
- [flow-reporting](#)
- [no flow-reporting](#)
- [passphrase page](#)
- [no passphrase page](#)
- [passphrase password](#)
- [no passphrase password](#)
- [passphrase active-time](#)
- [confirm page](#)
- [no confirm page](#)
- [confirm active-time](#)
- [consent required](#)
- [no consent required](#)
- [consent user-idle-timeout](#)

- [consent optional page-url](#)
- [no consent optional page-url](#)
- [consent mandatory page-url](#)
- [no consent mandatory page-url](#)
- [consent mandatory address](#)
- [no consent mandatory address](#)
- [custom-header insertion](#)
- [no custom-header insertion](#)
- [custom-header entry](#)
- [no custom-header entry](#)
- [no custom-header entries](#)
- [reporting](#)
- [profile](#)
- [packet-monitor](#)
- [no packet-monitor](#)
- [user-actions](#)
- [block-page dropped-connections](#)
- [no block-page dropped-connections](#)
- [block-details](#)
- [no block-details](#)
- [block-page object](#)
- [bypass-ss0](#)
- [no bypass-ss0](#)
- [tcp timeout](#)
- [udp timeout](#)
- [fragments](#)
- [no fragments](#)
- [bypass-server-to-client-inspection](#)
- [no bypass-server-to-client-inspection](#)
- [sip](#)
- [no sip](#)
- [h323](#)
- [no h323](#)
- [unauthenticated-redirect](#)
- [no unauthenticated-redirect](#)
- [ecli/dos-policy.cdl](#)
 - [no dos-policy uuid](#)
 - [no dos-policies](#)
 - [dos-policy uuid](#)
 - [clone dos-policy](#)
 - [clear dos-policy](#)
 - [clear dos-policies statistics](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [priority](#)
 - [enable](#)
 - [no enable](#)
 - [comment](#)
 - [no comment](#)
 - [destination address](#)
 - [source address](#)
 - [ip-version](#)
 - [service](#)
 - [schedule](#)
 - [action](#)
 - [action-profile](#)
 - [ticket tag1](#)
 - [no ticket tag1](#)
 - [ticket tag2](#)
 - [no ticket tag2](#)
 - [ticket tag3](#)
 - [no ticket tag3](#)
- [ecli/website-object.cdl](#)
 - [no website-objects](#)
 - [no website-groups](#)
 - [no website-object](#)
 - [no website-group](#)
 - [website-object](#)
 - [clone website-object](#)
 - [name](#)
 - [domain](#)
 - [no domain](#)
 - [uuid](#)
 - [no uuid](#)
 - [website-group](#)
 - [clone website-group](#)
 - [name](#)
 - [website-object](#)
 - [no website-object](#)
 - [website-group](#)
 - [no website-group](#)
 - [no website-group-members](#)
 - [uuid](#)
 - [no uuid](#)
- [ecli/decryption-policy.cdl](#)
 - [no decryption-policy](#)
 - [no decryption-policies](#)

- [decryption-policy](#)
- [clone decryption-policy](#)
- [uuid](#)
- [no uuid](#)
- [name](#)
- [no name](#)
- [priority](#)
- [comment](#)
- [no comment](#)
- [enable](#)
- [no enable](#)
- [source address](#)
- [destination address](#)
- [service](#)
- [users included](#)
- [match-operation](#)
- [web-category](#)
- [web-site](#)
- [country](#)
- [schedule](#)
- [action](#)
- [ticket](#)
- [no ticket](#)
- [ip-type](#)
- [clear decryption-policy](#)
- [clear decryption-policies](#)
- [ecli/country-object.cdl](#)
 - [no country-group](#)
 - [no country-groups](#)
 - [country-group](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [no country](#)
 - [no countries](#)
 - [country](#)
 - [no country-group](#)
 - [no country-groups](#)
 - [country-group](#)
- [ecli/security-policy.cdl](#)
 - [security-policies max-count](#)
 - [no security-policies](#)
 - [no security-policy ipv4](#)
 - [security-policy ipv4](#)
 - [no security-policy ipv6](#)
 - [security-policy ipv6](#)
 - [clone security-policy ipv4](#)
 - [clone security-policy ipv6](#)
 - [clear security-policies statistics](#)
 - [clear security-policy ipv4](#)
 - [clear security-policy ipv6](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [priority](#)
 - [no priority](#)
 - [comment](#)
 - [no comment](#)
 - [enable](#)
 - [no enable](#)
 - [from](#)
 - [to](#)
 - [source address](#)
 - [destination address](#)
 - [service](#)
 - [source port](#)
 - [users](#)
 - [match-operation](#)
 - [application](#)
 - [and-all-matched-applications](#)
 - [no and-all-matched-applications](#)
 - [web-category](#)
 - [url-list](#)
 - [custom-match](#)
 - [country](#)
 - [schedule](#)
 - [action](#)
 - [action-profile](#)
 - [no action-profile](#)
 - [ticket tag1](#)
 - [no ticket tag1](#)
 - [ticket tag2](#)
 - [no ticket tag2](#)
 - [ticket tag3](#)
 - [no ticket tag3](#)
 - [policy section](#)
 - [no policy section](#)
 - [no policy sections](#)
 - [uuid](#)

- [name](#)
- [ecli/web-category-object.cdl](#)
 - [no web-category-groups](#)
 - [no web-category-group](#)
 - [web-category-group](#)
 - [name](#)
 - [web-category-object](#)
 - [no web-category-object](#)
 - [web-category-group](#)
 - [no web-category-group](#)
 - [no web-category-group-members](#)
 - [uuid](#)
 - [no uuid](#)
- [ecli/threat-prevention-object.cdl](#)
 - [no threat-prevention-profile](#)
 - [no threat-prevention-profiles](#)
 - [threat-prevention-profile](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [negate](#)
 - [no negate](#)
 - [no threat-prevention-object](#)
 - [no threat-prevention-objects](#)
 - [threat-prevention-object](#)
- [ecli/policies-settings.cdl](#)
 - [policies-setting](#)
 - [enforcement](#)
 - [block-connections application-signatures-unavailable](#)
 - [no block-connections application-signatures-unavailable](#)
 - [block-connections malware-databases-not-downloaded](#)
 - [no block-connections malware-databases-not-downloaded](#)
 - [active-application-caching](#)
 - [no active-application-caching](#)
 - [cached-application-bypass](#)
 - [no cached-application-bypass](#)
 - [application-cache default](#)
 - [no application-cache default timeout](#)
 - [application-cache global timeout](#)
 - [no application-cache global timeout](#)
 - [application-cache global threshold](#)
 - [no application-cache global threshold](#)
 - [clear app-cache](#)
 - [block-connections geoip-database-not-downloaded](#)
 - [no block-connections geoip-database-not-downloaded](#)
 - [block-connections botnet-signature-not-unavailable](#)
 - [no block-connections botnet-signature-not-unavailable](#)
 - [ssl-server-inspection](#)
 - [no ssl-server-inspection](#)
 - [bypass-decryption cfs-not-licensed](#)
 - [no bypass-decryption cfs-not-licensed](#)
 - [bypass-decryption cfs-fail-connect](#)
 - [no bypass-decryption cfs-fail-connect](#)
 - [bypass-decryption geoip-database-not-downloaded](#)
 - [no bypass-decryption geoip-database-not-downloaded](#)
 - [policy-based-dos-protection](#)
 - [no policy-based-dos-protection](#)
 - [app-custom-malware-mode](#)
 - [application-based-on](#)
 - [threat-based-on](#)
 - [antispyware-based-on](#)
 - [antivirus-based-on](#)
 - [geoip-mode](#)
 - [geoip-inspection-based-on](#)
 - [botnet-mode](#)
 - [dpissl-mode](#)
 - [dpissh-mode](#)
 - [dos-mode](#)
 - [syn-flood](#)
 - [udp-flood](#)
 - [icmp-flood](#)
 - [attack](#)
 - [ddos](#)
 - [threat-profile-for-zone](#)
 - [based-on](#)
 - [prevent enable](#)
 - [no prevent enable](#)
 - [prevent profile](#)
 - [packet-monitor enable](#)
 - [no packet-monitor enable](#)
 - [packet-monitor profile](#)
 - [log enable](#)
 - [no log enable](#)
 - [log profile](#)
 - [log redundancy](#)
 - [no log redundancy](#)
 - [high-priority](#)
 - [medium-priority](#)
 - [low-priority](#)

- [no high-priority](#)
- [no medium-priority](#)
- [no low-priority](#)
- [antispyware-profile-for-zone](#)
- [inbound](#)
- [no inbound](#)
- [outbound](#)
- [no outbound](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [http-clientless-notification](#)
- [no http-clientless-notification](#)
- [based-on](#)
- [prevent](#)
- [no prevent](#)
- [packet-monitor](#)
- [no packet-monitor](#)
- [log enable](#)
- [no log enable](#)
- [log redundancy](#)
- [no log redundancy](#)
- [high-danger](#)
- [medium-danger](#)
- [low-danger](#)
- [no high-danger](#)
- [no medium-danger](#)
- [no low-danger](#)
- [antivirus-profile-for-zone](#)
- [cloud](#)
- [no cloud](#)
- [inbound](#)
- [no inbound](#)
- [outbound](#)
- [no outbound](#)
- [prevent](#)
- [no prevent](#)
- [packet-monitor](#)
- [no packet-monitor](#)
- [log enable](#)
- [no log enable](#)
- [log redundancy](#)
- [no log redundancy](#)
- [password-protected-zip](#)
- [no password-protected-zip](#)
- [ms-office-macros](#)
- [no ms-office-macros](#)
- [packed-executables](#)
- [no packed-executables](#)
- [smtp-responses](#)
- [no smtp-responses](#)
- [eicar-detection](#)
- [no eicar-detection](#)
- [http-byte-range](#)
- [no http-byte-range](#)
- [ftp-rest](#)
- [no ftp-rest](#)
- [scan-high-compression](#)
- [no scan-high-compression](#)
- [ecli/block-page.cdl](#)
 - [no block-page](#)
 - [no block-pages](#)
 - [block-page](#)
 - [name](#)
 - [block-details](#)
 - [no block-details](#)
 - [alert-text](#)
 - [no alert-text](#)
 - [logo-icon](#)
- [ecli/application-object.cdl](#)
 - [no application-group](#)
 - [no application-groups](#)
 - [application-group](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)
 - [no application](#)
 - [no applications](#)
 - [application](#)
 - [no application-group](#)
 - [no application-groups](#)
 - [application-group](#)
- [ecli/reporting-profile.cdl](#)
 - [no reporting-profile](#)
 - [no reporting-profiles](#)
 - [reporting-profile](#)
 - [clone reporting-profile](#)
 - [name](#)
 - [uuid](#)
 - [no uuid](#)

- [frequency](#)
- [no frequency](#)
- [log-monitor](#)
- [no log-monitor](#)
- [email-alert](#)
- [no email-alert](#)
- [email-address](#)
- [no email-address](#)
- [syslog](#)
- [no syslog](#)
- [syslog-profile](#)
- [no syslog-profile](#)
- [ipfix](#)
- [no ipfix](#)
- [color](#)
- [event matched](#)
- [no event matched](#)
- [event begin](#)
- [no event begin](#)
- [event end](#)
- [no event end](#)
- [ecli/dos-action-profile.cdl](#)
 - [no dos-action-profile](#)
 - [no dos-action-profiles](#)
 - [dos-action-profile](#)
 - [clone dos-action-profile](#)
 - [uuid](#)
 - [no uuid](#)
 - [name](#)
 - [no name](#)
 - [syn-flood-protection enable](#)
 - [no syn-flood-protection enable](#)
 - [syn-flood-protection mode](#)
 - [syn-attack-threshold](#)
 - [no syn-attack-threshold](#)
 - [tcp-sack](#)
 - [no tcp-sack](#)
 - [limit-mss](#)
 - [no limit-mss](#)
 - [log-syn-packets](#)
 - [no log-syn-packets](#)
 - [syn-flood-blacklisting](#)
 - [no syn-flood-blacklisting](#)
 - [blacklist-threshold](#)
 - [never-blacklist-wan](#)
 - [no never-blacklist-wan](#)
 - [management](#)
 - [no management](#)
 - [udp-flood-protection](#)
 - [no udp-flood-protection](#)
 - [udp-flood-attack threshold](#)
 - [no udp-flood-attack threshold](#)
 - [udp-flood-attack block-timeout](#)
 - [no udp-flood-attack block-timeout](#)
 - [icmp-flood-protection](#)
 - [no icmp-flood-protection](#)
 - [icmp-flood-attack threshold](#)
 - [no icmp-flood-attack threshold](#)
 - [icmp-flood-attack block-timeout](#)
 - [no icmp-flood-attack block-timeout](#)
 - [ddos protection](#)
 - [no ddos protection](#)
 - [ddos threshold](#)
 - [no ddos threshold](#)
 - [ddos fliter-bypass-rate](#)
 - [no ddos fliter-bypass-rate](#)
 - [ddos allow-list-timeout](#)
 - [no ddos allow-list-timeout](#)
 - [ddos on-wan-interfaces](#)
 - [no ddos on-wan-interfaces](#)
 - [ddos management](#)
 - [no ddos management](#)
 - [spank-protection](#)
 - [no spank-protection](#)
 - [smurf-protection](#)
 - [no smurf-protection](#)
 - [land-attack-protection](#)
 - [no land-attack-protection](#)
 - [connection-limit enable](#)
 - [no connection-limit enable](#)
 - [connection-limit maximum](#)
 - [connection-limit destination](#)
 - [no connection-limit destination](#)
 - [connection-limit source](#)
 - [no connection-limit source](#)
- [ecli/custom-match.cdl](#)
 - [no custom-match](#)
 - [no custom-matches](#)
 - [custom-match](#)
 - [clone custom-match](#)

- [no custom-match-group](#)
- [no custom-match-groups](#)
- [custom-match-group](#)
- [clone custom-match-group](#)
- [name](#)
- [no name](#)
- [uuid](#)
- [no uuid](#)
- [no custom-match](#)
- [no custom-matches](#)
- [custom-match](#)
- [no custom-match-group](#)
- [no custom-match-groups](#)
- [custom-match-group](#)
- [name](#)
- [no name](#)
- [uuid](#)
- [no uuid](#)
- [type](#)
- [match-object](#)
- [mail-from included](#)
- [mail-from excluded](#)
- [no mail-from](#)
- [rcpt-to included](#)
- [rcpt-to excluded](#)
- [no rcpt-to](#)
- [connection-side](#)
- [direction](#)
- [ecli/security-action-profile_show.cdl](#)
 - [show security-action-profiles](#)
 - [show security-action-profile](#)
- [ecli/dos-policy_show.cdl](#)
 - [show dos-policies](#)
 - [show dos-policy uuid](#)
- [ecli/website-object_show.cdl](#)
 - [show website-objects](#)
 - [show website-object](#)
 - [show website-groups](#)
 - [show website-group](#)
- [ecli/decryption-policy_show.cdl](#)
 - [show decryption-policies](#)
 - [show decryption-policy](#)
- [ecli/country-object_show.cdl](#)
 - [show countries](#)
 - [show country](#)
 - [show country-groups](#)
 - [show country-group](#)
- [ecli/security-policy_show.cdl](#)
 - [show security-policies](#)
 - [show security-policy ipv4](#)
 - [show security-policy ipv6](#)
 - [show policy](#)
- [ecli/web-category-object_show.cdl](#)
 - [show web-category-objects](#)
 - [show web-category-groups](#)
 - [show web-category-group](#)
- [ecli/threat-prevention-object_show.cdl](#)
 - [show threat-prevention-profiles](#)
 - [show threat-prevention-profile](#)
- [ecli/policies-settings_show.cdl](#)
 - [show policies-settings base](#)
- [ecli/block-page_show.cdl](#)
 - [show block-pages](#)
 - [show block-page](#)
- [ecli/application-object_show.cdl](#)
 - [show application-groups](#)
 - [show application-group](#)
- [ecli/reporting-profile_show.cdl](#)
 - [show reporting-profiles](#)
 - [show reporting-profile](#)
- [ecli/dos-action-profile_show.cdl](#)
 - [show dos-action-profiles](#)
 - [show dos-action-profile](#)
- [ecli/custom-match_show.cdl](#)
 - [show custom-matches](#)
 - [show custom-match](#)
 - [show custom-match-groups](#)
 - [show custom-match-group](#)
- [ecli/switch-controller.cdl](#)

- [switch-controller](#)
- [port](#)
- [clear-statistics switch](#)
- [enable](#)
- [no enable](#)
- [port-description](#)
- [no port-description](#)
- [link-speed](#)
- [stp](#)
- [no stp](#)
- [poe](#)
- [no poe](#)
- [portshield-uplink](#)
- [no portshield-uplink](#)
- [portshield-uplink-secondary](#)
- [no portshield-uplink-secondary](#)
- [poe-priority](#)
- [poe-limit-type](#)
- [power-limit](#)
- [no power-limit](#)
- [port-isolation](#)
- [no port-isolation](#)
- [voice-vlan](#)
- [no voice-vlan](#)
- [voice-vlan-cos-mode](#)
- [cos-value](#)
- [trust](#)
- [no trust](#)
- [bandwidth-ingress](#)
- [no bandwidth-ingress](#)
- [bandwidth-egress](#)
- [no bandwidth-egress](#)
- [security-count](#)
- [no security-count](#)
- [storm-control broadcast](#)
- [no storm-control broadcast](#)
- [storm-control unknown-multicast](#)
- [no storm-control unknown-multicast](#)
- [storm-control unknown-unicast](#)
- [no storm-control unknown-unicast](#)
- [port-8021x config](#)
- [port-8021x reauth](#)
- [no port-8021x reauth](#)
- [port-8021x reauth-period](#)
- [port-8021x guest-vlan](#)
- [no port-8021x guest-vlan](#)
- [port-8021x radius-vlan-assignment](#)
- [no port-8021x radius-vlan-assignment](#)
- [portshield](#)
- [no portshield](#)
- [native-vlan](#)
- [no native-vlan](#)
- [vlan-trunk](#)
- [no vlan-trunk](#)
- [vlan-list](#)
- [no vlan-list](#)
- [switch](#)
- [name](#)
- [authorize](#)
- [restart](#)
- [upgrade](#)
- [model](#)
- [no switch](#)
- [serial](#)
- [comment](#)
- [ip](#)
- [user-name](#)
- [password](#)
- [active-partition](#)
- [switch-mode](#)
- [uplink](#)
- [firewall-uplink](#)
- [no firewall-uplink](#)
- [management](#)
- [uplink-secondary](#)
- [management-secondary](#)
- [parent-switch-name](#)
- [parent-switch-uplink](#)
- [no parent-switch-uplink](#)
- [stp-mode](#)
- [stp](#)
- [no stp](#)
- [switch-8021x](#)
- [no switch-8021x](#)
- [switch-8021x-guest-vlan](#)
- [no switch-8021x-guest-vlan](#)
- [switch-8021x-guest-vlan-id](#)
- [jumbo-frame-size](#)
- [voice-vlan](#)
- [state](#)
- [vlan](#)
- [priority-tag](#)

- [dscp](#)
- [radius](#)
- [no radius](#)
- [authorized-port](#)
- [key-string](#)
- [timeout-reply](#)
- [retry](#)
- [user](#)
- [no user](#)
- [password](#)
- [privilege-type](#)
- [network](#)
- [no network](#)
- [ip](#)
- [dns primary](#)
- [no dns primary](#)
- [dns secondary](#)
- [no dns secondary](#)
- [route](#)
- [no route](#)
- [arp](#)
- [no arp](#)
- [port](#)
- [arp-aging-time](#)
- [aging-time](#)
- [qos](#)
- [enable](#)
- [no enable](#)
- [schedule-method](#)
- [trust-mode](#)
- [round-robin-weight1](#)
- [no round-robin-weight1](#)
- [round-robin-weight2](#)
- [no round-robin-weight2](#)
- [round-robin-weight3](#)
- [no round-robin-weight3](#)
- [round-robin-weight4](#)
- [no round-robin-weight4](#)
- [round-robin-weight5](#)
- [no round-robin-weight5](#)
- [round-robin-weight6](#)
- [no round-robin-weight6](#)
- [round-robin-weight7](#)
- [no round-robin-weight7](#)
- [round-robin-weight8](#)
- [no round-robin-weight8](#)
- [qos-dscp](#)
- [dscp-id](#)
- [qos-cos](#)
- [cos-id](#)
- [ecli/switch-controller_show.cd](#)
 - [show switch-controller switch](#)
 - [show switch-controller voice-vlan](#)
 - [show switch-controller user](#)
 - [show switch-controller port](#)
 - [show switch-controller network](#)
 - [show switch-controller radius](#)
 - [show switch-controller route](#)
 - [show switch-controller arp](#)
 - [show switch-controller arp-aging-time](#)
 - [show switch-controller qos](#)
 - [show switch-controller qos-dscp](#)
 - [show switch-controller qos-cos](#)
- [ecli/dell-switch.cd](#)
 - [dell-switch](#)
 - [port](#)
 - [clear-statistics switch](#)
 - [enable](#)
 - [no enable](#)
 - [link-speed](#)
 - [stp](#)
 - [no stp](#)
 - [poe](#)
 - [no poe](#)
 - [portshield-uplink](#)
 - [no portshield-uplink](#)
 - [portshield-uplink-secondary](#)
 - [no portshield-uplink-secondary](#)
 - [poe-priority](#)
 - [power-limit](#)
 - [no power-limit](#)
 - [portshield](#)
 - [no portshield](#)
 - [vlan-trunk](#)
 - [no vlan-trunk](#)
 - [vlan-list](#)
 - [no vlan-list](#)
 - [switch](#)
 - [switch-restart](#)
 - [model](#)

- [no switch](#)
- [serial](#)
- [comment](#)
- [ip](#)
- [user-name](#)
- [password](#)
- [switch-mode](#)
- [uplink](#)
- [firewall-uplink](#)
- [no firewall-uplink](#)
- [management](#)
- [parent-switch-id](#)
- [parent-switch-uplink](#)
- [no parent-switch-uplink](#)
- [uplink-secondary](#)
- [management-secondary](#)
- [stp-mode](#)
- [stp](#)
- [no stp](#)
- [poe-threshold](#)
- [poe-traps](#)
- [no poe-traps](#)
- [power-limit-type](#)
- [poe-management-mode](#)
- [poe-detection-type](#)
- [ecli/dell-switch_show.cdl](#)
 - [show dell-switch switch](#)
 - [show dell-switch port](#)
 - [show dell-switch statistics switch](#)
 - [show dell-switch firmware-mgmt switch](#)
 - [show dell-switch ports](#)
 - [show dell-switch status](#)
 - [show dell-switch product-info](#)
- [ecli/wireless.cdl](#)
 - [wireless](#)
 - [radio-role](#)
 - [enable](#)
 - [no enable](#)
 - [ssid](#)
 - [short-guard-interval](#)
 - [no short-guard-interval](#)
 - [aggregation](#)
 - [no aggregation](#)
 - [threshold fragmentation](#)
 - [threshold rts](#)
 - [authentication-type](#)
 - [wep-key](#)
 - [no wep-key](#)
 - [eapol-version](#)
 - [wpa cipher-type](#)
 - [wpa passphrase](#)
 - [no wpa passphrase](#)
 - [connect](#)
 - [scan](#)
 - [wireless-interface-as-wan](#)
 - [no wireless-interface-as-wan](#)
 - [connectivity-check](#)
 - [no connectivity-check](#)
 - [remote-ip](#)
 - [no remote-ip](#)
 - [antenna-diversity](#)
 - [restore-default](#)
 - [block-station](#)
 - [allow-station](#)
 - [disassociate-station](#)
 - [disassociate-stations](#)
 - [schedule](#)
 - [country-code](#)
 - [radio mode](#)
 - [radio band](#)
 - [channel](#)
 - [virtual-access-point group](#)
 - [no virtual-access-point group](#)
 - [wpa group-key](#)
 - [no wpa group-key](#)
 - [radius retries](#)
 - [radius retry-interval](#)
 - [no radius retry-interval](#)
 - [radius server](#)
 - [no radius server](#)
 - [hide-ssid](#)
 - [no hide-ssid](#)
 - [interval beacon](#)
 - [green-ap enable](#)
 - [no green-ap enable](#)
 - [green-ap timeout](#)
 - [high-throughput](#)
 - [no high-throughput](#)
 - [short-slot-time](#)
 - [no short-slot-time](#)

- [antenna-diversity](#)
- [transmit-power](#)
- [preamble-length](#)
- [interval dtim](#)
- [association-timeout](#)
- [max-clients](#)
- [data-rate](#)
- [no protection mode](#)
- [protection mode](#)
- [protection rate](#)
- [protection type](#)
- [restore-default](#)
- [access-list](#)
- [no access-list](#)
- [wds](#)
- [no wds](#)
- [station](#)
- [enable](#)
- [no enable](#)
- [access-point ssid](#)
- [no access-point ssid](#)
- [access-point authentication-type](#)
- [access-point cipher-type](#)
- [no access-point passphrase](#)
- [access-point passphrase](#)
- [no vlan-id](#)
- [vlan-id](#)
- [wireless-interface-as-wan](#)
- [no wireless-interface-as-wan](#)
- [wds](#)
- [no wds](#)
- [ids](#)
- [rogue-access-point-detection](#)
- [no rogue-access-point-detection](#)
- [authorized-access-point](#)
- [schedule](#)
- [no schedule](#)
- [authorizing-access-point](#)
- [scan](#)
- [ecli/sonicpoint.cdl](#)
 - [sonicpoint](#)
 - [register sonicpoint](#)
 - [firmware-management](#)
 - [override-download-url sonicpoint n](#)
 - [no override-download-url sonicpoint n](#)
 - [override-download-url sonicpoint nv](#)
 - [no override-download-url sonicpoint nv](#)
 - [override-download-url sonicpoint ndr](#)
 - [no override-download-url sonicpoint ndr](#)
 - [override-download-url sonicpoint ac](#)
 - [no override-download-url sonicpoint ac](#)
 - [override-download-url sonicwave400](#)
 - [no override-download-url sonicwave400](#)
 - [override-download-url sonicwave200](#)
 - [no override-download-url sonicwave200](#)
 - [reset sonicpoint](#)
 - [reset sonicpoint-n](#)
 - [reset sonicpoint-nv](#)
 - [reset sonicpoint-ndr](#)
 - [reset sonicpoint-ac](#)
 - [reset sonicwave400](#)
 - [reset sonicwave200](#)
 - [upload sonicpoint](#)
 - [upload sonicpoint-n](#)
 - [upload sonicpoint-nv](#)
 - [upload sonicpoint-ndr](#)
 - [upload sonicpoint-ac](#)
 - [upload sonicwave400](#)
 - [upload sonicwave200](#)
 - [synchronize](#)
 - [reboot](#)
 - [no sonicpoint](#)
 - [no profile](#)
 - [no sonicpoints](#)
 - [no profiles](#)
 - [sonicpoint](#)
 - [profile](#)
 - [enable](#)
 - [no enable](#)
 - [rf-monitoring](#)
 - [no rf-monitoring](#)
 - [poe-out](#)
 - [no poe-out](#)
 - [low-power](#)
 - [no low-power](#)
 - [retain](#)
 - [no retain](#)
 - [led](#)
 - [no led](#)
 - [name-prefix](#)
 - [name](#)

- [country-code](#)
- [eapol-version](#)
- [band-steering](#)
- [no band-steering](#)
- [sslvpn](#)
- [no sslvpn](#)
- [radius](#)
- [no radius](#)
- [administrator](#)
- [no administrator](#)
- [wldp-sensor](#)
- [no wldp-sensor](#)
- [wwan](#)
- [no wwan](#)
- [connection-profile](#)
- [enable](#)
- [no enable](#)
- [country](#)
- [no country](#)
- [service-provider](#)
- [no service-provider](#)
- [plan-type](#)
- [no plan-type](#)
- [connection-type](#)
- [no connection-type](#)
- [dialed-number](#)
- [no dialed-number](#)
- [user-name](#)
- [no user-name](#)
- [user-password](#)
- [no user-password](#)
- [apn](#)
- [no apn](#)
- [mesh](#)
- [no mesh](#)
- [ble](#)
- [no ble](#)
- [packet-capture](#)
- [mode](#)
- [band](#)
- [channel](#)
- [capture](#)
- [no capture](#)
- [ssid](#)
- [no ssid](#)
- [bssid](#)
- [no bssid](#)
- [mac](#)
- [no mac](#)
- [radio](#)
- [radio-2400mhz](#)
- [radio-5000mhz](#)
- [virtual-access-point group](#)
- [no virtual-access-point group](#)
- [dynamic-vlan](#)
- [no dynamic-vlan](#)
- [vlan](#)
- [no vlan](#)
- [no vlans](#)
- [enable](#)
- [no enable](#)
- [schedule](#)
- [mode](#)
- [dfs-channel](#)
- [no dfs-channel](#)
- [ssid](#)
- [no ssid](#)
- [channel](#)
- [band](#)
- [short-guard-interval](#)
- [no short-guard-interval](#)
- [aggregation](#)
- [no aggregation](#)
- [mimo](#)
- [no mimo](#)
- [no access-list](#)
- [access-list](#)
- [mic-failure acl-blacklist](#)
- [no mic-failure acl-blacklist](#)
- [mic-failure frequency](#)
- [virtual-access-point wep-key](#)
- [no virtual-access-point wep-key](#)
- [authentication-type](#)
- [no wep-key](#)
- [wep-key](#)
- [wpa auth-balance-method](#)
- [wpa cipher-type](#)
- [wpa group-key-interval](#)
- [wpa passphrase](#)
- [no wpa passphrase](#)
- [wpa pmf](#)
- [no wpa pmf](#)

- [remote-mac-access-control](#)
- [no remote-mac-access-control](#)
- [hide-ssid](#)
- [no hide-ssid](#)
- [ids-scan schedule](#)
- [no ids-scan schedule](#)
- [data-rate](#)
- [transmit-power](#)
- [antenna-diversity](#)
- [interval](#)
- [threshold](#)
- [max-clients](#)
- [station-inactivity-timeout](#)
- [preamble-length](#)
- [protection mode](#)
- [no protection mode](#)
- [protection rate](#)
- [protection type](#)
- [short-slot-time](#)
- [no short-slot-time](#)
- [deny-b](#)
- [no deny-b](#)
- [wds-ap](#)
- [no wds-ap](#)
- [wmm](#)
- [no wmm](#)
- [green-ap enable](#)
- [no green-ap enable](#)
- [green-ap timeout](#)
- [rssi enable](#)
- [no rssi enable](#)
- [rssi threshold](#)
- [airtime-fairness](#)
- [no airtime-fairness](#)
- [80211r](#)
- [no 80211r](#)
- [80211k neighbour-report](#)
- [no 80211k neighbour-report](#)
- [80211v](#)
- [no 80211v](#)
- [ids](#)
- [scan sonicpoint](#)
- [scan all](#)
- [authorizing-access-point](#)
- [widp](#)
- [enable](#)
- [no enable](#)
- [authorized-access-point](#)
- [rogue-access-point](#)
- [unauthorized-access-point](#)
- [no unauthorized-access-point](#)
- [arp-cache-lookup](#)
- [no arp-cache-lookup](#)
- [active-probe](#)
- [no active-probe](#)
- [evil-twin](#)
- [no evil-twin](#)
- [block-traffic](#)
- [no block-traffic](#)
- [disassociate rogue](#)
- [no disassociate rogue](#)
- [disassociate krack](#)
- [no disassociate krack](#)
- [rf-monitoring](#)
- [measurement-interval](#)
- [management-frame-flood](#)
- [no management-frame-flood](#)
- [null-probe-response](#)
- [no null-probe-response](#)
- [broadcasting-deauthentication](#)
- [no broadcasting-deauthentication](#)
- [station-with-invalid-ssid](#)
- [no station-with-invalid-ssid](#)
- [wellenreiter](#)
- [no wellenreiter](#)
- [ad-hoc-station](#)
- [no ad-hoc-station](#)
- [long-duration](#)
- [no long-duration](#)
- [unassociated-station](#)
- [no unassociated-station](#)
- [netstumbler](#)
- [no netstumbler](#)
- [eapol-packet-flood](#)
- [no eapol-packet-flood](#)
- [weak-wep-iv](#)
- [no weak-wep-iv](#)
- [watch station](#)
- [no watch station](#)
- [clear rf-monitoring statistics](#)
- [fairnet enable](#)
- [no fairnet enable](#)

- [fairnet policy](#)
- [no fairnet policy](#)
- [no fairnet policies](#)
- [enable](#)
- [no enable](#)
- [direction](#)
- [range](#)
- [interface](#)
- [rate min](#)
- [rrm](#)
- [enable](#)
- [no enable](#)
- [sta threshold](#)
- [radio threshold](#)
- [dcs](#)
- [dcsscheme24g](#)
- [dcsscheme5g](#)
- [force-switch](#)
- [ecli/wifi-multimedia.cdl](#)
 - [wmm profile](#)
 - [no wmm profile](#)
 - [no wmm profiles](#)
 - [name](#)
 - [no access-point](#)
 - [access-point](#)
 - [no station](#)
 - [station](#)
 - [no mapping](#)
 - [mapping](#)
- [ecli/floor-plan.cdl](#)
 - [floor-plan](#)
 - [no floor-plan](#)
 - [no floor-plans](#)
 - [name](#)
 - [comment](#)
 - [no comment](#)
 - [image](#)
 - [no image](#)
 - [image-width](#)
 - [no image-width](#)
 - [image-height](#)
 - [no image-height](#)
 - [scale](#)
 - [no scale](#)
 - [export floor-plan](#)
 - [import floor-plan](#)
 - [access-point](#)
 - [no access-point](#)
 - [no access-points](#)
- [ecli/virtual-access-point.cdl](#)
 - [virtual-access-point group](#)
 - [virtual-access-point profile](#)
 - [virtual-access-point object](#)
 - [no virtual-access-point](#)
 - [name](#)
 - [virtual-access-point](#)
 - [no virtual-access-point](#)
 - [no virtual-access-points](#)
 - [virtual-access-point group](#)
 - [virtual-access-point profile](#)
 - [virtual-access-point object](#)
 - [no virtual-access-point](#)
 - [name](#)
 - [virtual-access-point](#)
 - [group](#)
 - [no virtual-access-point](#)
 - [no group](#)
 - [no virtual-access-points](#)
 - [no groups](#)
 - [name](#)
 - [schedule](#)
 - [access-list](#)
 - [no access-list](#)
 - [radio-type](#)
 - [max-clients](#)
 - [wep-key](#)
 - [authentication-type](#)
 - [wpa auth-balance-method](#)
 - [cipher-type](#)
 - [no cipher-type](#)
 - [wpa passphrase](#)
 - [no wpa passphrase](#)
 - [wpa group-key-interval](#)
 - [wpa pmf](#)
 - [no wpa pmf](#)
 - [radius](#)
 - [no radius](#)
 - [remote-mac-access-control](#)
 - [no remote-mac-access-control](#)

- [wds](#)
- [no wds](#)
- [allow-b](#)
- [no allow-b](#)
- [radio-type](#)
- [ssid](#)
- [no ssid](#)
- [no vlan-id](#)
- [vlan-id](#)
- [suppress-ssid](#)
- [no suppress-ssid](#)
- [enable](#)
- [no enable](#)
- [dynamic-vlan](#)
- [no dynamic-vlan](#)
- [vlan](#)
- [no vlan](#)
- [no vlans](#)
- [profile](#)
- [no profile](#)
- [80211r](#)
- [no 80211r](#)
- [80211k neighbour-report](#)
- [no 80211k neighbour-report](#)
- [80211v](#)
- [no 80211v](#)
- ecli/wireless_show.cdl
 - [show wireless](#)
- ecli/sonicpoint_show.cdl
 - [show sonicpoint](#)
- ecli/virtual-assist.cdl
 - [virtual-assist](#)
 - [logout](#)
 - [assistance-code](#)
 - [no assistance-code](#)
 - [support-without-invitation](#)
 - [no support-without-invitation](#)
 - [disclaimer](#)
 - [no disclaimer](#)
 - [customer-access-link](#)
 - [no customer-access-link](#)
 - [link-on-portal-login](#)
 - [no link-on-portal-login](#)
 - [technician-email-list](#)
 - [no technician-email-list](#)
 - [invitation-subject](#)
 - [no invitation-subject](#)
 - [invitation-message](#)
 - [no invitation-message](#)
 - [max-requests](#)
 - [limit-message](#)
 - [no limit-message](#)
 - [max-requests-one-ip](#)
 - [no max-requests-one-ip](#)
 - [pending-request-expiration](#)
 - [no pending-request-expiration](#)
 - [deny-requests](#)
 - [no deny-requests](#)
- ecli/virtual-assist_show.cdl
 - [show virtual-assist](#)

Syntax

clear

Mode

All Modes

Description

Reset functions.

Syntax

export

Mode

All Modes

Description

Export system status or configuration.

Syntax

no

Mode

All Modes

Description

Negate a command or set its defaults.

Syntax

show

Mode

All Modes

Description

Show system status or configuration.

Syntax

cancel

Mode

All Modes
Top Level

Description

Cancel current changes and return to the previous mode.

Example

cancel

Syntax

commit [best-effort]

Mode

All Modes
Top Level
Dos Policy
Decryption Policy
Security Policy
Security Policy IPv6

Description

Commits configuration changes.

Options

best-effort Commits only valid configuration (best effort).

Example

commit

Syntax

commit-with-exit

Mode

Guest User Generate
Dos Policy
Decryption Policy
Security Policy
Security Policy IPv6

Description

Commits configuration changes and exit to up level mode.

Example

commit-with-exit

Syntax

end

Mode

Config

Description

End configuration mode.

Example

end

Syntax

end

Mode

All Modes
Top Level
Config

Description

Exits current mode and returns to global configuration mode.

Example

end

Syntax

exit

Mode

All Modes

Description

Exit the current mode.

Example

```
exit
```

Syntax

```
help
```

Mode

All Modes

Description

Display command help.

Example

```
help
```

Syntax

```
configure [ terminal ]
```

Mode

Top Level

Description

Enter configuration mode.

Options

terminal Terminal.

Example

```
configure
```

Syntax

```
no pending-config
```

Mode

Config

Syntax

```
dbg
```

Mode

Config

Description

Enter debug setting mode.

Example

Syntax

```
cli idle-timeout default <CLI_IDLE_TIMEOUT>
```

Mode

Config

Description

Set the maximum time that a session can be idle before being logged off.

Options

<CLI_IDLE_TIMEOUT>	Integer in the form: D OR 0xHH. Max: 60 Example: 5

Example

```
cli idle-timeout default 5
```

Syntax

```
cli screen width default <CLI_SCREEN_WIDTH>
```

Mode

Config

Description

Set the number of characters on a line.

Options

<CLI_SCREEN_WIDTH>	Integer in the form: D OR 0xHHHH. Min: 80 Max: 2560 Example: 80

Example

```
cli screen width default 80
```

Syntax

```
cli screen length default <CLI_SCREEN_LENGTH>
```

Mode

Config

Description

Set the number of lines on screen.

Options

<CLI_SCREEN_LENGTH>	Integer in the form: D OR 0xHHHH. Min: 24 Max: 1600 Example: 24

Example

```
cli screen length default 24
```

Syntax

cli show-unmodified default

Mode

Config

Description

Show unmodified pending configuration changes.

Example

cli show-unmodified default

Syntax

no cli show-unmodified default

Mode

Config

Description

Hide unmodified pending configuration changes.

Example

no cli show-unmodified default

Syntax

cli pager default

Mode

Config

Description

Enable cli pager.

Example

cli pager default

Syntax

no cli pager default

Mode

Config

Description

Disable cli pager.

Example

no cli pager default

Syntax

```
cli interactive-prompts default
```

Mode

Config

Description

Enable cli interactive prompts.

Example

```
cli interactive-prompts default
```

Syntax

```
no cli interactive-prompts default
```

Mode

Config

Description

Disable cli interactive prompts.

Example

```
no cli interactive-prompts default
```

Syntax

```
cli ftp user default <WORD>
```

Mode

Config

Description

Configure the username for File Transfer Protocol (FTP) connections.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli ftp user default Administrator
```

Syntax

```
no cli ftp user default
```

Mode

Config

Description

Configure anonymous username for File Transfer Protocol (FTP) connections.

Example

```
cli ftp user default
```

Syntax

```
cli ftp password default <ENC_PASSWORD>
```

Mode

Config

Description

Configure the password for File Transfer Protocol (FTP) connections.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
cli ftp password default mysecret
```

Syntax

```
no cli ftp password default
```

Mode

Config

Description

Clear password for File Transfer Protocol (FTP) connections.

Example

```
no cli ftp password default
```

Syntax

```
cli banner { connection <WORD> | login <WORD> | logout <WORD> }
```

Mode

Config

Description

CLI banner configuration.

Options

- connection** Configure connection banner
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- login** Configure login banner
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- logout** Configure logout banner
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli banner connection "You have connected to System 88.\nLog in using a valid username and password combination."\ncli banner login "You are now logged into System 88.\nPlease do not make modifications without proper authorization."\ncli banner logout "Thank you for visiting System 88.\nLogin is now terminated."
```

Syntax

```
no cli banner { connection | login | logout }
```

Mode

Config

Description

Clear CLI banner message.

Options

connection Clear connection banner

login Clear login banner

logout Clear logout banner

Example

```
no cli banner connection
no cli banner login
no cli banner logout
```

Syntax

```
clear screen
```

Mode

All Modes

Description

Disable command history for the current CLI session.

Example

```
clear screen
```

Syntax

```
no cli history
```

Mode

All Modes

Description

Disable command history for the current CLI session.

Example

```
no cli history
```

Syntax

```
cli history [ size <UINT32> ]
```

Mode

All Modes

Description

Enable command history for the current CLI session.

Options

- size** Command history buffer size.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

cli history

Syntax

cli format out { json | plain-text }

Mode

All Modes

Description

Set the CLI format.

Options

- json** Render all CLI output as JSON.
- plain-text** Render all CLI output as plain-text.

Example

cli format out plain-text

Syntax

cli api-json indent

Mode

All Modes

Description

Indent the json returned by api.

Options

- indent** Indent the json returned by api.

Example

cli api-json indent

Syntax

no cli api-json indent

Mode

All Modes

Description

Don't indent the json returned by api.

Options

indent Don't indent the json returned by api.

Example

```
no cli api-json indent
```

Syntax

```
cli idle-timeout session <CLI_IDLE_TIMEOUT>
```

Mode

All Modes

Description

Set the maximum time that a session can be idle before being logged off.

Options

<CLI_IDLE_TIMEOUT> Integer in the form: D OR 0xHH.
Max: 60
Example: 5

Example

```
cli idle-timeout session 5
```

Syntax

```
cli screen width session <CLI_SCREEN_WIDTH>
```

Mode

All Modes

Description

Set the number of characters on a line.

Options

<CLI_SCREEN_WIDTH> Integer in the form: D OR 0xHHHH.
Min: 80
Max: 2560
Example: 80

Example

```
cli screen width session 80
```

Syntax

```
cli screen length session <CLI_SCREEN_LENGTH>
```

Mode

All Modes

Description

Set the number of lines on screen.

Options

<CLI_SCREEN_LENGTH> Integer in the form: D OR 0xHHHH.

Min: 24
Max: 1600
Example: 24

Example

```
cli screen-length session 24
```

Syntax

```
cli show-unmodified session
```

Mode

Config

Description

Show unmodified pending configuration changes.

Example

```
cli show-unmodified session
```

Syntax

```
no cli show-unmodified session
```

Mode

Config

Description

Hide unmodified pending configuration changes.

Example

```
no cli show-unmodified session
```

Syntax

```
cli pager session
```

Mode

All Modes

Description

Enable cli pager.

Example

```
cli pager session
```

Syntax

```
no cli pager session
```

Mode

All Modes

Description

Disable cli pager.

Example

```
no cli pager session
```

Syntax

```
cli interactive-prompts session
```

Mode

All Modes

Description

Enable cli interactive prompts.

Example

```
cli interactive-prompts session
```

Syntax

```
no cli interactive-prompts session
```

Mode

All Modes

Description

Disable cli interactive prompts.

Example

```
no cli interactive-prompts session
```

Syntax

```
cli data-store index [ keys-only ]
```

Mode

All Modes

Options

keys-only

Syntax

```
no cli data-store index
```

Mode

All Modes

Syntax

```
cli ftp user session <WORD>
```

Mode

All Modes

Description

Configure the username for File Transfer Protocol (FTP) connections.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cli ftp user session Administrator
```

Syntax

```
no cli ftp user session
```

Mode

All Modes

Description

Configure anonymous username for File Transfer Protocol (FTP) connections.

Example

```
cli ftp user session
```

Syntax

```
cli ftp password session <ENC_PASSWORD>
```

Mode

All Modes

Description

Configure the password for File Transfer Protocol (FTP) connections.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
cli ftp password session mysecret
```

Syntax

```
no cli ftp password session
```

Mode

All Modes

Description

Clear password for File Transfer Protocol (FTP) connections.

Example

```
no cli ftp password session
```

Syntax

show current-config [with-pending-config]

Mode

All Modes
Top Level
Config

Description

Show current configuration.

Options

with-pending-config View current configuration with pending changes included in the output.

Example

show current-config

Syntax

show current-config [{ custom | default }] [with-pending-config]

Mode

Top Level
Config

Description

Show current configuration.

Options

- custom*** Show custom configuration.
- default*** Show system/factory default configuration.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show current-config

Syntax

show pending-config

Mode

All Modes
Top Level

Description

Show pending configuration.

Example

show pending-config

Syntax

show cli [banner | data-model [{ group <INT32> | tag <WORD> }] | data-store [group <INT32>] | debug | ftp | history [top <UINT16>] | idle-timeout | interactive-prompts | pager | screen | show-api | show-unmodified | staging-area [{ command-hash | current-mode }] | token-types]

Mode

All Modes

Description

Show a list of recent commands issued.

Options

<i>banner</i>	Show CLI Banner.
<i>data-model</i>	Display data model debug information.
<i>group</i> <INT32>	Group ID. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
<i>tag</i> <WORD>	CGI tag name. Word in the form: WORD or \"QUOTED STRING\". Example: abc
<i>data-store</i> <i>group</i> <INT32>	Display data store debug information. Group ID. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
<i>debug</i>	Display CLI debug information.
<i>ftp</i>	Display CLI FTP configuration.
<i>history</i> <i>top</i> <UINT16>	Show a list of recent keywords issued. Show the specified number of recent keywords issued. Integer in the form: D OR 0xHHHH. Example: 123
<i>idle-timeout</i>	Show idle timeout.
<i>interactive-prompts</i>	show cli interactive prompts.
<i>pager</i>	Show tty pager.
<i>screen</i>	Show screen settings.
<i>show-api</i>	Display Show command API debug information.
<i>show-unmodified</i>	Show unmodified settings.
<i>staging-area</i>	Display staging area debug information.
<i>command-hash</i>	Display only the command hash.
<i>current-mode</i>	Display only the current mode.
<i>token-types</i>	Display token type debug information.

Example

show cli history

Syntax

check-network { content-filters | default-gateway | dns-server1 | dns-server2 | dns-server3 | license-manager | my-sonicwall }

Mode

Top Level
Config

Description

check network settings.

Options

<i>content-filters</i>	check network settings content-filters.
<i>default-gateway</i>	check network settings default gateway.
<i>dns-server1</i>	check network settings dns server1.
<i>dns-server2</i>	check network settings dns server2.
<i>dns-server3</i>	check network settings dns server3.
<i>license-manager</i>	check network settings license-manager.
<i>my-sonicwall</i>	check network settings my-sonicwall.

Example

```
check-network default-gateway
```

Syntax

```
ping <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ] [ ipv6-preferred ]
```

Mode

Top Level
Config

Description

Ping the specified host.

Options

<i><HOSTNAME_MIXED></i>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n
<i>interface</i>	Route ping request through the specified interface.
<i><WAN_MGMT_INTERFACE></i>	WAN interface name. Example: X1
<i>ipv6-preferred</i>	Prefer to use IPv6 network.

Example

```
ping 10.10.10.1
ping fe00::1 ipv6-preferred
ping 10.10.10.1 interface X1
```

Syntax

```
traceroute <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ] [ ipv6-preferred ]
```

Mode

Top Level
Config

Description

Traceroute to the specified host.

Options

<i><HOSTNAME_MIXED></i>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

<i>interface</i>	Route traceroute request through the specified interface.
<i><WAN_MGMT_INTERFACE></i>	WAN interface name. Example: <i>X1</i>
<i>ipv6-preferred</i>	Prefer to use IPv6 network.

Example

```
traceroute 10.10.10.1
traceroute fe00::1
traceroute www.sonicwall.com
traceroute 10.10.10.1 interface X1
```

Syntax

```
diag network-path <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Find network path of the specified IP address.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Example

```
diag network-path 10.10.10.1
diag network-path fe00::1
```

Syntax

```
network-path <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Find network path of the specified IP address.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Example

```
network-path 10.10.10.1
network-path fe00::1
```

Syntax

```
nslookup <HOSTNAME> [ ipv4 | ipv6 ] [ customized [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

DNS lookup of the specified host.

Options

<HOSTNAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
ipv4	DNS lookup IPv4 host.
ipv6	DNS lookup IPv6 host.
customized	DNS lookup customized host.
ipv4-dns	IPv4 DNS server.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
ipv6-dns	IPv6 DNS server.
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
nslookup 1001::1001 ipv6 customized ipv4-dns 10.10.10.1
nslookup ipv6.baidu.com ipv6 customized ipv6-dns 1001::1001
nslookup 10.10.10.1
nslookup www.sonicwall.com
```

Syntax

```
diag reverse-lookup <IP_V4V6_HOST> [ ipv6 [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

Resolve the specified reverse name.

Options

<IP_V4V6_HOST>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
ipv6	DNS lookup IPv6 host.
ipv4-dns	IPv4 DNS server.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
ipv6-dns	IPv6 DNS server.
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
diag reverse-lookup 1001::1001 ipv6 ipv4-dns 10.10.10.1
diag reverse-lookup 10.10.10.1
```

Syntax

```
reverse-lookup <IP_V4V6_HOST> [ ipv6 [ ipv4-dns <IPV4_HOST> ] [ ipv6-dns <IPV6_HOST> ] ]
```

Mode

Top Level
Config

Description

Resolve the specified reverse name.

Options

<IP_V4V6_HOST>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
ipv6	DNS lookup IPv6 host.

<i>ipv4-dns</i>	IPv4 DNS server.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>ipv6-dns</i>	IPv6 DNS server.
<i><IPV6_HOST></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
reverse-lookup 1001::1001 ipv6 ipv4-dns 10.10.10.1
reverse-lookup 10.10.10.1
```

Syntax

```
diag rbl-lookup ip <IPV4_HOST> domain <HOSTNAME> dns-server <IPV4_HOST>
```

Mode

Top Level
Config

Description

Lookup the specified realtime black list.

Options

<i>ip</i>	RBL IP address.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>domain</i>	RBL domain name.
<i><HOSTNAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
<i>dns-server</i>	RBL DNS server.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
diag rbl-lookup ip 10.10.10.1 domain domainName dns-server 10.10.10.22
```

Syntax

```
rbl-lookup ip <IPV4_HOST> domain <HOSTNAME> dns-server <IPV4_HOST>
```

Mode

Top Level
Config

Description

Lookup the specified realtime black list.

Options

<i>ip</i>	RBL IP address.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>domain</i>	RBL domain name.
<i><HOSTNAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
<i>dns-server</i>	RBL DNS server.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
rbl-lookup ip 10.10.10.1 domain domainName dns-server 10.10.10.22
```

Syntax

```
diag mxlookup <HOSTNAME_MIXED> [ port <IPV4_PORT> ]
```

Mode

Top Level
Config

Description

MX lookup and banner check the specified domain name and SMTP port.

Options

<HOSTNAME_MIXED>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:3257:9652\n</i>
port	Specified the SMTP port.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
diag mxlookup 10.10.10.1 port 25
diag mxlookup fe00::1
diag mxlookup www.sonicwall.com
```

Syntax

```
mxlookup <HOSTNAME_MIXED> [ port <IPV4_PORT> ]
```

Mode

Top Level
Config
Anti-Spam

Description

MX lookup and banner check the specified domain name and SMTP port.

Options

<HOSTNAME_MIXED>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:3257:9652\n</i>
port	Specified the SMTP port.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
mxlookup 10.10.10.1 port 25
mxlookup fe00::1
mxlookup www.sonicwall.com
```

Syntax

```
diag geo-botnet-lookup <IP_V4V6_HOST>
```

Mode

Top Level
Config

Description

Check GEO location and lookup BOTNET server.

Options

<IP_V4V6_HOST>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>

Example

```
diag geo-botnet-lookup 10.10.10.1
```

Syntax

```
geo-botnet-lookup <IP_V4V6_HOST>
```

Mode

Top Level
Config
Geo-IP
Botnet

Description

Check GEO location and lookup BOTNET server.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
geo-botnet-lookup 10.10.10.1
```

Syntax

```
pmtu-discovery <HOSTNAME_MIXED> [ interface <WAN_MGMT_INTERFACE> ]
```

Mode

Top Level
Config

Description

Path MTU discovery to the specified host.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n
interface Path MTU discovery request through the specified interface.
<WAN_MGMT_INTERFACE> WAN interface name.
Example: X1

Example

```
pmtu-discovery 10.10.10.1  
pmtu-discovery 1001::1001  
pmtu-discovery 10.10.10.1 interface X1
```

Syntax

```
diag show abrentries <IP_V4V6_HOST>
```

Mode

All Modes

Description

Look Up ABR Entries By Destination IP.

Options

<IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example

```
diag show abrentries 10.10.10.1
diag show abrentries 1001::1001
```

Syntax

```
diag show processes
```

Mode

All Modes

Description

Show all system processes.

Example

```
diag show processes
```

Syntax

```
diag show process <WORD>
```

Mode

All Modes

Description

Show a system process.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
diag show process tNtp
```

Syntax

```
diag show multicore
```

Mode

All Modes

Description

Show multicore utilization information.

Example

```
diag show multicore
```

Syntax

```
diag show build-info
```

Mode

All Modes

Description

Show build information.

Example

```
diag show build-info
```

Syntax

```
diag show cpu
```

Mode

All Modes

Description

Show all cpu information.

Example

```
diag show cpu
```

Syntax

```
diag show web-server
```

Mode

All Modes

Description

Show all web server information.

Example

```
diag show web-server
```

Syntax

```
diag show ssh-server
```

Mode

All Modes

Description

Show all ssh server connection information.

Example

```
diag show ssh-server
```

Syntax

```
diag show mem-pools
```

Mode

All Modes

Description

Show mem-pools information.

Example

```
diag show mem-pools
```

Syntax

```
diag show memory [ summary | verbose ] [ period <UINT32> [ repeat-forever | repeats <UINT32> ] [ on-console ] ]
```

Mode

All Modes

Description

Show memory information.

Options

summary	Show just a short memory usage summary.
verbose	Show verbose output including top memory usage reports.
period	Keep showing the information periodically.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
repeat-forever	Repeat forever (or until canceled by 'diag no show memory period').
repeats	Stop after a number of periodic showings.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
on-console	Print the periodic output to the console. Note this will not be terminated on logout.

Example

```
diag show memory
diag show memory summary
diag show memory verbose
diag show memory period 2 repeats 10
diag show memory verbose period 2 repeat-forever on-console
```

Syntax

```
diag no show memory period
```

Mode

All Modes

Description

Stop periodic printing of memory information.

Options

period	Period.

Example

```
diag no show memory period
```

Syntax

```
diag show timer-counters
```

Mode

All Modes

Description

Show timer counters.

Example

```
diag show timer-counters
```

Syntax

```
diag show wd-stats
```

Mode

All Modes

Description

Show watchdog statistics.

Example

```
diag show wd-stats
```

Syntax

```
diag clear pp-stats
```

Mode

All Modes

Description

Clear packet processing statistics.

Example

```
diag clear pp-stats
```

Syntax

```
diag show pp-stats [ full ]
```

Mode

All Modes

Description

Show packet processing statistics.

Options

full Full statistics.

Example

```
diag show pp-stats
```

Syntax

```
diag clear active-utm
```

Mode

All Modes

Description

Clear active UTM statistics.

Example

diag clear active-utm

Syntax

diag show active-utm

Mode

All Modes

Description

Show active UTM statistics.

Example

diag show active-utm

Syntax

diag show debug interface <INTERFACE_NAME>

Mode

All Modes

Description

Show interface debug information.

Options

<INTERFACE_NAME> Interface name.
Example: *X0*

Example

diag show debug interface "X1"

Syntax

diag test memory { sw } { alloc <UINT32> | double-free [delay <UINT32>] | free }

Mode

All Modes

Description

Test memory allocation and free.

Options

sw	SonicWall memory allocation tests.
alloc	Test memory allocation.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

<i>double-free</i>	Test memory double-free.
<i>delay</i>	Delay in seconds before the 2nd free.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
<i>free</i>	Test memory free.

Example

```
diag test memory sw alloc 64
diag test memory sw free
diag test memory sw double-free
diag test memory sw double-free delay 30
```

Syntax

```
diag show alerts [ top <UINT32> ]
```

Mode

All Modes

Description

Show alerts.

Options

<i>top</i>	Maximum alerts to display.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
diag show alerts
diag show alerts top 100
```

Syntax

```
diag show log [ top <UINT32> ]
```

Mode

All Modes

Description

Show log entries.

Options

<i>top</i>	Maximum entries to display.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
diag show log
diag show log top 100
```

Syntax

```
diag show drop-stats
```

Mode

All Modes

Description

Show packet drop statistics.

Example

```
diag show drop-stats
```

Syntax

```
diag show pktio-nic
```

Mode

All Modes

Description

Show packet pktio nic statistics.

Example

```
diag show pktio-nic
```

Syntax

```
diag show pktio-throughput-start interface <PHYS_INTERFACE>
```

Mode

All Modes

Description

Show pktio throughput.

Options

<i>interface</i>	Specify one interface.
<i><PHYS_INTERFACE></i>	Physical interface name. Example: <i>X0</i>

Example

```
diag show pktio-throughput-start interface X0
```

Syntax

```
diag show pktio-throughput-stop
```

Mode

All Modes

Description

Show pktio throughput stop.

Example

```
diag show pktio-throughput stop
```

Syntax

```
diag cli pager-test
```

Mode

All Modes

Description

CLI pager test.

Example

```
diag cli pager-test
```

Syntax

```
diag show switch port { counters | status } [ interface <PHYS_INTERFACE> ]
```

Mode

All Modes

Description

Show switch diagnostics information.

Options

counters	Show port counters information.
status	Show port status information.
interface	Show switch diagnostics information for the specified interface.
<PHYS_INTERFACE>	Physical interface name. Example: <i>X0</i>

Example

```
diag show switch port status
diag show switch port status interface "X1"
diag show switch port counters
diag show switch port counters interface "X1"
```

Syntax

```
diag gen-coredump
```

Mode

All Modes

Description

Stop SonicOS and generate a coredump.

Example

```
diag gen-coredump
```

Syntax

```
diag ipv6-check-network-settings { default-gateway | license-manager | mysonicwall }
```

Mode

All Modes

Description

Check ipv6 network settings.

Options

default-gateway Test the ipv6 default gateway.

license-manager Test the ipv6 license manager domain

mysonicwall Test the ipv6 mysonicwall domain

Example

```
diag ipv6-check-network-settings
```

Syntax

```
diag cfs-lookup <WORD>
```

Mode

All Modes

Description

Check CFS lookup for particular ip.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
diag cfs-lookup www.abcd.com
```

Syntax

```
diag purge-coredump
```

Mode

All Modes

Description

Purge the all coredump files.

Example

```
diag purge-coredump
```

Syntax

```
diag advanced unified-policy-engine { policy-based-security-services | policy-mode-switching }
```

Mode

Config

Description

Enable Unified policy engine settings.

Options

policy-based-security-services Ability to Enable or Disable Policy-based Security Services.

policy-mode-switching Allow Policy Mode Switching.

Example

```
diag advanced unified-policy-engine policy-mode-switching
```

Syntax

```
no diag advanced unified-policy-engine { policy-based-security-services | policy-mode-switching }
```

Mode

Config

Description

Disable Unified policy engine settings.

Options

policy-based-security-services Disable Ability to Enable or Disable Policy-based Security Services.

policy-mode-switching Disable Policy Mode Switching.

Example

```
no diag advanced unified-policy-engine policy-mode-switching
```

Syntax

```
diag advanced arp
```

Mode

Config

Description

Configure advanced diag ARP settings.

Example

```
diag advanced arp
```

Syntax

```
bridging
```

Mode

Diag Advanced ARP Settings

Description

Enable ARP bridging.

Example

```
bridging
```

Syntax

```
no bridging
```

Mode

Diag Advanced ARP Settings

Description

Disable ARP bridging.

Example

```
no bridging
```

Syntax

```
open-arp-behavior
```

Mode

Diag Advanced ARP Settings

Description

Enable open ARP behavior (WARNING: Insecure!!).

Example

```
open-arp-behavior
```

Syntax

```
no open-arp-behavior
```

Mode

Diag Advanced ARP Settings

Description

Disable open ARP behavior.

Example

```
no open-arp-behavior
```

Syntax

```
source-ip-validation
```

Mode

Diag Advanced ARP Settings

Description

Enable source IP address validation for being directly connected.

Example

```
source-ip-validation
```

Syntax

```
no source-ip-validation
```

Mode

Diag Advanced ARP Settings

Description

Disable source IP address validation for being directly connected.

Example

no source-ip-validation

Syntax

only-unicast

Mode

Diag Advanced ARP Settings

Description

Enable only allowing ARP entries with unicast addresses.

Example

only-unicast

Syntax

no only-unicast

Mode

Diag Advanced ARP Settings

Description

Disable only allowing ARP entries with unicast addresses.

Example

no only-unicast

Syntax

limit-nonresponsive

Mode

Diag Advanced ARP Settings

Description

Enable limiting ARPs of non-responsive IPs.

Example

limit-nonresponsive

Syntax

no limit-nonresponsive

Mode

Diag Advanced ARP Settings

Description

Disable limiting ARPs of non-responsive IPs.

Example

no limit-nonresponsive

Syntax

```
redundant-ip-resolution-rate [ amount <UINT16> ]
```

Mode

Diag Advanced ARP Settings

Description

Enable protection against ARP storm.

Options

amount Set limit for ARP sending rate when resolve a same ip, protect against ARP storm.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
redundant-ip-resolution-rate amount 10
```

Syntax

```
no redundant-ip-resolution-rate
```

Mode

Diag Advanced ARP Settings

Description

Disable protection against ARP storm.

Example

```
no redundant-ip-resolution-rate
```

Syntax

```
update-exist-arp
```

Mode

Diag Advanced ARP Settings

Description

Enable update exist ARP entry when gratuitous ARP received on a L2 bridge interface.

Example

```
update-exist-arp
```

Syntax

```
no update-exist-arp
```

Mode

Diag Advanced ARP Settings

Description

Disable update exist ARP entry when gratuitous ARP received on a L2 bridge interface.

Example

```
no update-exist-arp
```

Syntax

bypass-for-l2bridge

Mode

Diag Advanced ARP Settings

Description

Enable bypassing ARP processing on L2 bridge interfaces.

Example

bypass-for-l2bridge

Syntax

no bypass-for-l2bridge

Mode

Diag Advanced ARP Settings

Description

Disable bypassing ARP processing on L2 bridge interfaces.

Example

no bypass-for-l2bridge

Syntax

gratuitous-arp-compatibility

Mode

Diag Advanced ARP Settings

Description

Enable gratuitous ARP compatibility mode.

Example

gratuitous-arp-compatibility

Syntax

no gratuitous-arp-compatibility

Mode

Diag Advanced ARP Settings

Description

Disable gratuitous ARP compatibility mode.

Example

no gratuitous-arp-compatibility

Syntax

secondary-subnet

Mode

Diag Advanced ARP Settings

Description

Enable ARP responses for secondary subnets on WAN Interfaces.

Example

secondary-subnet

Syntax

no secondary-subnet

Mode

Diag Advanced ARP Settings

Description

Disable ARP responses for secondary subnets on WAN Interfaces.

Example

no secondary-subnet

Syntax

gratuitous-arp-limit [amount <UINT32>]

Mode

Diag Advanced ARP Settings

Description

Enable gratuitous ARP limiting and never broadcast more than set number gratuitous ARPs in any 60 second period.

Options

amount Set limit of gratuitous ARPs in any 60 second period.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

gratuitous-arp-limit amount 100

Syntax

no gratuitous-arp-limit

Mode

Diag Advanced ARP Settings

Description

Disable gratuitous ARP limiting.

Example

no gratuitous-arp-limit

Syntax

```
system-broadcast [ interval <UINT32> ]
```

Mode

Diag Advanced ARP Settings

Description

Enable periodically broadcast system ARPs and set the interval.

Options

interval Set the interval for periodically broadcast system ARPs in minutes.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
system-broadcast interval 60
```

Syntax

```
no system-broadcast
```

Mode

Diag Advanced ARP Settings

Description

Disable periodically broadcast system ARPs.

Example

```
no system-broadcast
```

Syntax

```
ignore-arps-with-primary-mac-from-other-if
```

Mode

Diag Advanced ARP Settings

Description

Enable ignore ARPs with primary-gateway's MAC received on other interfaces.

Example

```
ignore-arps-with-primary-mac-from-other-if
```

Syntax

```
no ignore-arps-with-primary-mac-from-other-if
```

Mode

Diag Advanced ARP Settings

Description

Disable ignore ARPs with primary-gateway's MAC received on other interfaces.

Example

```
no ignore-arp-with-primary-mac-from-other-if
```

Syntax

```
display-mac-tracking
```

Mode

Diag Advanced ARP Settings

Description

Enable displaying of MAC tracking information.

Example

```
display-mac-tracking
```

Syntax

```
no display-mac-tracking
```

Mode

Diag Advanced ARP Settings

Description

Disable displaying of MAC tracking information.

Example

```
no display-mac-tracking
```

Syntax

```
send system-arp
```

Mode

Diag Advanced ARP Settings

Description

Send system ARPs.

Example

```
send system-arp
```

Syntax

```
diag advanced network
```

Mode

Config

Description

Configure advanced diag Network and Routing settings.

Example

```
diag advanced network
```

Syntax

flush-alternate-path-flows

Mode

Diag Advanced Network Settings

Description

Enable flushing flows on alternate path when normal route path is enabled (affects existing connections).

Example

flush-alternate-path-flows

Syntax

no flush-alternate-path-flows

Mode

Diag Advanced Network Settings

Description

Disable flushing flows on alternate path when normal route path is enabled (affects existing connections).

Example

no flush-alternate-path-flows

Syntax

update-route-version

Mode

Diag Advanced Network Settings

Description

Enable updating route version when route is enabled/disabled (affects existing connections).

Example

update-route-version

Syntax

no update-route-version

Mode

Diag Advanced Network Settings

Description

Disable updating route version when route is enabled/disabled (affects existing connections).

Example

no update-route-version

Syntax

tcp-packet-option-tagging

Mode

Diag Advanced Network Settings

Description

Enable TCP packet option tagging.

Example

tcp-packet-option-tagging

Syntax

no tcp-packet-option-tagging

Mode

Diag Advanced Network Settings

Description

Disable TCP packet option tagging.

Example

no tcp-packet-option-tagging

Syntax

fix-malformed-tcp-headers

Mode

Diag Advanced Network Settings

Description

Enable fix/ignore malformed TCP headers.

Example

fix-malformed-tcp-headers

Syntax

no fix-malformed-tcp-headers

Mode

Diag Advanced Network Settings

Description

Disable fix/ignore malformed TCP headers.

Example

no fix-malformed-tcp-headers

Syntax

sequence-number-randomization

Mode

Diag Advanced Network Settings

Description

Enable TCP sequence number randomization.

Example

```
sequence-number-randomization
```

Syntax

```
no sequence-number-randomization
```

Mode

Diag Advanced Network Settings

Description

Disable TCP sequence number randomization.

Example

```
no sequence-number-randomization
```

Syntax

```
syn-validation
```

Mode

Diag Advanced Network Settings

Description

Enable performing SYN validation when not operating in strict TCP compliance mode.

Example

```
syn-validation
```

Syntax

```
no syn-validation
```

Mode

Diag Advanced Network Settings

Description

Disable performing SYN validation when not operating in strict TCP compliance mode.

Example

```
no syn-validation
```

Syntax

```
clear ospf
```

Mode

Diag Advanced Network Settings

Description

Clear OSPF process.

Example

```
clear ospf
```

Syntax

```
debounce-interface-state-changes
```

Mode

Diag Advanced Network Settings

Description

Enable Debounce Interface State Changes for routing protocols.

Example

```
debounce-interface-state-changes
```

Syntax

```
no debounce-interface-state-changes
```

Mode

Diag Advanced Network Settings

Description

Disable Debounce Interface State Changes for routing protocols.

Example

```
no debounce-interface-state-changes
```

Syntax

```
clear dont-fragment-bit
```

Mode

Diag Advanced Network Settings

Description

Enable clear DF (don't fragment) bit.

Example

```
clear dont-fragment-bit
```

Syntax

```
no clear dont-fragment-bit
```

Mode

Diag Advanced Network Settings

Description

Disable clear DF (don't fragment) bit.

Example

```
no clear dont-fragment-bit
```

Syntax

```
smaller-first-fragment
```

Mode

Diag Advanced Network Settings

Description

Enable smaller first fragment packets.

Example

```
smaller-first-fragment
```

Syntax

```
no smaller-first-fragment
```

Mode

Diag Advanced Network Settings

Description

Disable smaller first fragment packets.

Example

```
no smaller-first-fragment
```

Syntax

```
ipv6-small-fragment
```

Mode

Diag Advanced Network Settings

Description

Enable IPv6 Fragmentation Packets smaller than 1280 bytes.

Example

```
ipv6-small-fragment
```

Syntax

```
no ipv6-small-fragment
```

Mode

Diag Advanced Network Settings

Description

Disable IPv6 Fragmentation Packets smaller than 1280 bytes.

Example

```
no ipv6-small-fragment
```

Syntax

override-mac

Mode

Diag Advanced Network Settings

Description

Enable override MAC address when NAT.

Example

override-mac

Syntax

no override-mac

Mode

Diag Advanced Network Settings

Description

Disable override MAC address when NAT.

Example

no override-mac

Syntax

drop-record-route

Mode

Diag Advanced Network Settings

Description

Enable dropping record route packets.

Example

drop-record-route

Syntax

no drop-record-route

Mode

Diag Advanced Network Settings

Description

Disable dropping record route packets.

Example

no drop-record-route

Syntax

dmz-icmp-redirect

Mode

Diag Advanced Network Settings

Description

Enable ICMP redirect on DMZ zone.

Example

dmz-icmp-redirect

Syntax

no dmz-icmp-redirect

Mode

Diag Advanced Network Settings

Description

Disable ICMP redirect on DMZ zone.

Example

no dmz-icmp-redirect

Syntax

enforce-strict-tcp-compliance-rfc5961

Mode

Diag Advanced Network Settings

Description

Enforce Strict TCP Compliance with RFC5961.

Example

enforce-strict-tcp-compliance-rfc5961

Syntax

no enforce-strict-tcp-compliance-rfc5961

Mode

Diag Advanced Network Settings

Description

Disable Enforce Strict TCP Compliance with RFC5961.

Example

no enforce-strict-tcp-compliance-rfc5961

Syntax

learning-bridge-filter

Mode

Diag Advanced Network Settings

Description

Enable learning-bridge filtering on L2 bridge interfaces.

Example

```
learning-bridge-filter
```

Syntax

```
no learning-bridge-filter
```

Mode

Diag Advanced Network Settings

Description

Disable learning-bridge filtering on L2 bridge interfaces.

Example

```
no learning-bridge-filter
```

Syntax

```
advertise-fqdn-route
```

Mode

Diag Advanced Network Settings

Description

Enable advertisement of FQDN based policy route to dynamic routing protocol.

Example

```
advertise-fqdn-route
```

Syntax

```
no advertise-fqdn-route
```

Mode

Diag Advanced Network Settings

Description

Disable advertisement of FQDN based policy route to dynamic routing protocol.

Example

```
no advertise-fqdn-route
```

Syntax

```
generate-interface-default-route
```

Mode

Diag Advanced Network Settings

Description

Generate an interface specific default route.

Example

```
generate-interface-default-route
```

Syntax

```
no generate-interface-default-route
```

Mode

Diag Advanced Network Settings

Description

Never generate an interface specific default route.

Example

```
no generate-interface-default-route
```

Syntax

```
zebos-granular-debug
```

Mode

Diag Advanced Network Settings

Description

Enable granular debug in routing protocols.

Example

```
zebos-granular-debug
```

Syntax

```
no zebos-granular-debug
```

Mode

Diag Advanced Network Settings

Description

Disable granular debug in routing protocols.

Example

```
no zebos-granular-debug
```

Syntax

```
diag advanced dns
```

Mode

Config

Description

Configure advanced diag DNS settings.

Example

```
diag advanced dns
```

Syntax

```
prefer-arpa
```

Mode

Diag Advanced DNS Settings

Description

Enable prefer arpa as suffix when commit ipv6 DNS reverse name resolution.

Example

```
prefer-arpa
```

Syntax

```
no prefer-arpa
```

Mode

Diag Advanced DNS Settings

Description

Disable prefer arpa as suffix when commit ipv6 DNS reverse name resolution.

Example

```
no prefer-arpa
```

Syntax

```
stack-traffic-by-dp
```

Mode

Diag Advanced DNS Settings

Description

Enable stack traffic sending by DP core.

Example

```
stack-traffic-by-dp
```

Syntax

```
no stack-traffic-by-dp
```

Mode

Diag Advanced DNS Settings

Description

Disable stack traffic sending by DP core.

Example

```
no stack-traffic-by-dp
```

Syntax

diag advanced dns-proxy

Mode

Config

Description

Configure advanced diag DNS proxy settings.

Example

diag advanced dns-proxy

Syntax

request-size-percentage <UINT8>

Mode

Diag Advanced DNS Proxy Settings

Description

Configure the Percentage of proxy process ability.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

request-size-percentage 10

Syntax

support-fragmentation

Mode

Diag Advanced DNS Proxy Settings

Description

Enable Support fragmentation process on DNS packet.

Example

support-fragmentation

Syntax

no support-fragmentation

Mode

Diag Advanced DNS Proxy Settings

Description

Disable Support fragmentation process on DNS packet.

Example

no support-fragmentation

Syntax

server-failover-times <UINT32>

Mode

Diag Advanced DNS Proxy Settings

Description

Resolution failure times that trigger DNS server failover.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

server-failover-times 10

Syntax

no server-failover-times

Mode

Diag Advanced DNS Proxy Settings

Description

Resolution failure times that trigger DNS server failover.

Example

no server-failover-times

Syntax

cache-lifetime <UINT32>

Mode

Diag Advanced DNS Proxy Settings

Description

Lifetime of connection cache for DNS proxy packets.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

cache-lifetime 10

Syntax

no cache-lifetime

Mode

Diag Advanced DNS Proxy Settings

Description

Lifetime of connection cache for DNS proxy packets.

Example

```
no cache-lifetime
```

Syntax

```
dns-over-tcp
```

Mode

Diag Advanced DNS Proxy Settings

Description

Configure the DNS over TCP.

Example

```
dns-over-tcp
```

Syntax

```
no dns-over-tcp
```

Mode

Diag Advanced DNS Proxy Settings

Description

Configure the DNS over TCP.

Example

```
no dns-over-tcp
```

Syntax

```
exclude-vpn-traffic
```

Mode

Diag Advanced DNS Proxy Settings

Description

Exclude incoming VPN traffic from DNS Proxy processing.

Example

```
exclude-vpn-traffic
```

Syntax

```
no exclude-vpn-traffic
```

Mode

Diag Advanced DNS Proxy Settings

Description

Exclude incoming VPN traffic from DNS Proxy processing.

Example

```
no exclude-vpn-traffic
```

Syntax

```
diag advanced dns-security
```

Mode

Config

Description

Configure advanced diag DNS security settings.

Example

```
diag advanced dns-security
```

Syntax

```
dns-tunnel-minimum-packet-number <UINT32>
```

Mode

Diag Advanced DNS Security Settings

Description

Configure the minimum DNS packet number for DNS tunnel detection.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
dns-tunnel-minimum-packet-number 100
```

Syntax

```
dns-tunnel-ratio-threshold <UINT32>
```

Mode

Diag Advanced DNS Security Settings

Description

Configure the ratio threshold for corner DNS types.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
dns-tunnel-ratio-threshold 10
```

Syntax

dns-tunnel-number-threshold <UINT32>

Mode

Diag Advanced DNS Security Settings

Description

Configure the number threshold for normal DNS types.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

dns-tunnel-number-threshold 1000

Syntax

diag advanced dhcp

Mode

Config

Description

Configure advanced diag DHCP settings.

Example

diag advanced dhcp

Syntax

network-pre-discovery

Mode

Diag Advanced DHCP Settings

Description

Enable DHCP server network pre-discovery.

Example

network-pre-discovery

Syntax

no network-pre-discovery

Mode

Diag Advanced DHCP Settings

Description

Disable DHCP server network pre-discovery.

Example

no network-pre-discovery

Syntax

```
conflict-detect-period <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set the DHCP server conflict detect period in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
conflict-detect-period 300
```

Syntax

```
resources-to-discover <UINT8>
```

Mode

Diag Advanced DHCP Settings

Description

Set number of DHCP resources to discover.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
resources-to-discover 10
```

Syntax

```
conflicted-resource-timeout <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set the timeout for conflicted resource to be rechecked in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
conflicted-resource-timeout 1800
```

Syntax

```
available-resource-timeout <UINT16>
```

Mode

Description

Set the timeout for available resource to be rechecked in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
available-resource-timeout 600
```

Syntax

```
save leases
```

Mode

Diag Advanced DHCP Settings

Description

Save DHCP leases to flash.

Example

```
save leases
```

Syntax

```
dhcpnak
```

Mode

Diag Advanced DHCP Settings

Description

Enable sending DHCPNAK if the 'requested IP address' is on the wrong network.

Example

```
dhcpnak
```

Syntax

```
no dhcpnak
```

Mode

Diag Advanced DHCP Settings

Description

Disable sending DHCPNAK if the 'requested IP address' is on the wrong network.

Example

```
no dhcpnak
```

Syntax

```
lease-database-refresh-interval <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set time interval of DHCP lease database to be refreshed in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
lease_database_refresh_interval 600
```

Syntax

```
lease-database-refresh-number <UINT16>
```

Mode

Diag Advanced DHCP Settings

Description

Set number of DHCP leases in database to be refreshed.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
lease_database_refresh_number 10
```

Syntax

```
use-client-etherner-address
```

Mode

Diag Advanced DHCP Settings

Description

Enable use client Etherner address instead of client-identifier option.

Example

```
use-client-etherner-address
```

Syntax

```
no use-client-etherner-address
```

Mode

Diag Advanced DHCP Settings

Description

Disable use client Etherner address instead of client-identifier option.

Example

```
no use-client-etherner-address
```

Syntax

use-unicast-and-link-layer

Mode

Diag Advanced DHCP Settings

Description

Enable use unicast dst ip address and link-layer address when unicast flag is set.

Example

use-client-etherner-address

Syntax

no use-unicast-and-link-layer

Mode

Diag Advanced DHCP Settings

Description

Disable use unicast dst ip address and link-layer address when unicast flag is set.

Example

no use-unicast-and link-layer

Syntax

diag advanced voip

Mode

Config

Description

Configure advanced diag VoIP settings.

Example

diag advanced voip

Syntax

max-endpoints <UINT16>

Mode

Diag Advanced VoIP Settings

Description

Set the maximum 'public' VoIP endpoints.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

Syntax

no max-endpoints

Mode

Diag Advanced VoIP Settings

Description

Clear the maximum 'public' VoIP endpoints.

Example

no max-endpoints

Syntax

odd-media-control-port

Mode

Diag Advanced VoIP Settings

Description

Enable H323 use odd media control port.

Example

odd-media-control-port

Syntax

no odd-media-control-port

Mode

Diag Advanced VoIP Settings

Description

Disable H323 use odd media control port.

Example

no odd-media-control-port

Syntax

relax-quence-number-check

Mode

Diag Advanced VoIP Settings

Description

Enable relax sequence number checking for rtsp media streams.

Example

relax-quence-number-check

Syntax

```
no relax-quence-number-check
```

Mode

Diag Advanced VoIP Settings

Description

Disable relax sequence number checking for rtsp media streams.

Example

```
no relax-quence-number-check
```

Syntax

```
auto-add-sip
```

Mode

Diag Advanced VoIP Settings

Description

Enable auto-add SIP endpoints.

Example

```
auto-add-sip
```

Syntax

```
no auto-add-sip
```

Mode

Diag Advanced VoIP Settings

Description

Disable auto-add SIP endpoints.

Example

```
no auto-add-sip
```

Syntax

```
sip-transforms
```

Mode

Diag Advanced VoIP Settings

Description

Enable transforming SIP URIs to have an explicit port.

Example

```
sip-transforms
```

Syntax

```
no sip-transforms
```

Mode

Diag Advanced VoIP Settings

Description

Disable transforming SIP URIs to have an explicit port.

Example

```
no sip-transforms
```

Syntax

```
invite-flush
```

Mode

Diag Advanced VoIP Settings

Description

Enable flush active media for SIP INVITEs without SDP.

Example

```
flush-active-media
```

Syntax

```
no invite-flush
```

Mode

Diag Advanced VoIP Settings

Description

Disable flush active media for SIP INVITEs without SDP.

Example

```
no invite-flush
```

Syntax

```
invite-flush-unused
```

Mode

Diag Advanced VoIP Settings

Description

Enable flush unused media for SIP INVITEs without SDP.

Example

```
invite-flush-unused
```

Syntax

```
no invite-flush-unused
```

Mode

Diag Advanced VoIP Settings

Description

Disable flush unused media for SIP INVITEs without SDP.

Example

```
no invite-flush-unused
```

Syntax

```
reset sip-database
```

Mode

Diag Advanced VoIP Settings

Description

Reset sip database.

Example

```
reset sip-database
```

Syntax

```
bypass-sip-transformation
```

Mode

Diag Advanced VoIP Settings

Description

Enable bypass sip transformation over vpn.

Example

```
bypass-sip-transformation
```

Syntax

```
no bypass-sip-transformation
```

Mode

Diag Advanced VoIP Settings

Description

Disable bypass sip transformation over vpn.

Example

```
no bypass-sip-transformation
```

Syntax

```
enforce-access-rule-check
```

Mode

Diag Advanced VoIP Settings

Description

Enable enforce access rule checking on anticipated control sessions.

Example

```
enforce-access-rule-check
```

Syntax

```
no enforce-access-rule-check
```

Mode

Diag Advanced VoIP Settings

Description

Disable enforce access rule checking on anticipated control sessions.

Example

```
no enforce-access-rule-check
```

Syntax

```
diag advanced vpn
```

Mode

Config

Description

Configure advanced diag VPN settings.

Example

```
diag advanced vpn
```

Syntax

```
adjust-tcp-mss
```

Mode

Diag Advanced VPN Settings

Description

Enable adjusting TCP MSS option for VPN traffic.

Example

```
adjust-tcp-mss
```

Syntax

```
no adjust-tcp-mss
```

Mode

Diag Advanced VPN Settings

Description

Do not adjusting TCP MSS option for VPN traffic.

Example

```
no adjust-tcp-mss
```

Syntax

interoperable-ike-dh-exchange

Mode

Diag Advanced VPN Settings

Description

Enable using interoperable IKE DH exchange .

Example

interoperable-ike-dh-exchange

Syntax

no interoperable-ike-dh-exchange

Mode

Diag Advanced VPN Settings

Description

Disable using interoperable IKE DH exchange .

Example

no interoperable-ike-dh-exchange

Syntax

fragment-after-esp

Mode

Diag Advanced VPN Settings

Description

Enable fragmenting VPN packets after applying ESP.

Example

fragment-after-esp

Syntax

no fragment-after-esp

Mode

Diag Advanced VPN Settings

Description

Disable fragmenting VPN packets after applying ESP.

Example

no fragment-after-esp

Syntax

spi-cpi-parameter-index

Mode

Diag Advanced VPN Settings

Description

Enable using SPI/CPI parameter index for IPsec/IPcomp passthru connections.

Example

spi-cpi-parameter-index

Syntax

no spi-cpi-parameter-index

Mode

Diag Advanced VPN Settings

Description

Disable using SPI/CPI parameter index for IPsec/IPcomp passthru connections.

Example

no spi-cpi-parameter-index

Syntax

trust-built-in-ca

Mode

Diag Advanced VPN Settings

Description

Enable trust built-in CA certificates for IKE authentication and local certificate import.

Example

trust-built-in-ca

Syntax

no trust-built-in-ca

Mode

Diag Advanced VPN Settings

Description

Disable trust built-in CA certificates for IKE authentication and local certificate import.

Example

no trust-built-in-ca

Syntax

preserve-ike-port

Mode

Diag Advanced VPN Settings

Description

Enable preserve IKE port for pass through connections.

Example

```
preserve-ike-port
```

Syntax

```
no preserve-ike-port
```

Mode

Diag Advanced VPN Settings

Description

Disable preserve IKE port for pass through connections.

Example

```
no preserve-ike-port
```

Syntax

```
diag advanced encryption
```

Mode

Config

Description

Configure advanced diag encryption settings.

Example

```
diag advanced encryption
```

Syntax

```
hardware-encryption
```

Mode

Diag Advanced Encryption

Description

Enable hardware encryption.

Example

```
hardware-encryption
```

Syntax

```
no hardware-encryption
```

Mode

Diag Advanced Encryption

Description

Disable hardware encryption.

Example

```
no hardware-encryption
```

Syntax

```
ssl-v3
```

Mode

Diag Advanced Encryption

Description

Enable SSLv3.

Example

```
ssl-v3
```

Syntax

```
no ssl-v3
```

Mode

Diag Advanced Encryption

Description

Disable SSLv3.

Example

```
no ssl-v3
```

Syntax

```
tls-v1
```

Mode

Diag Advanced Encryption

Description

Enable TLSv1.

Example

```
tls-v1
```

Syntax

```
no tls-v1
```

Mode

Diag Advanced Encryption

Description

Disable TLSv1.

Example

```
no tls-v1
```

Syntax

```
diag advanced firewall
```

Mode

Config

Description

Configure advanced diag firewall settings.

Example

```
diag advanced firewall
```

Syntax

```
kill-cache-no-delay
```

Mode

All Modes

Description

Enable do not go to TIME_WAIT state when TCP 4-ways FIN completed.

Example

```
kill-cache-delay
```

Syntax

```
no kill-cache-no-delay
```

Mode

All Modes

Description

Disable do not go to TIME_WAIT state when TCP 4-ways FIN completed.

Example

```
no kill-cache-delay
```

Syntax

```
ftp-bounce-attack-protection
```

Mode

All Modes

Description

Enable FTP bounce attack protection.

Example

```
ftp-bounce-attack-protection
```

Syntax

no ftp-bounce-attack-protection

Mode

All Modes

Description

Disable FTP bounce attack protection.

Example

no ftp-bounce-attack-protection

Syntax

ftp-protocol-anomaly-attack-protection

Mode

All Modes

Description

Enable FTP protocol anomaly attack protection.

Example

ftp-protocol-anomaly-attack-protection

Syntax

no ftp-protocol-anomaly-attack-protection

Mode

All Modes

Description

Disable FTP protocol anomaly attack protection.

Example

no ftp-protocol-anomaly-attack-protection

Syntax

orphan-data-connection

Mode

All Modes

Description

Enable allow orphan data connections.

Example

orphan-data-connection

Syntax

no orphan-data-connection

Mode

All Modes

Description

Disable allow orphan data connections.

Example

no orphan-data-connection

Syntax

allow-zero-Port

Mode

All Modes

Description

Enable allow tcp/udp packet with source port being zero to pass through firewall.

Example

allow-zero-Port

Syntax

no allow-zero-Port

Mode

All Modes

Description

Disable allow tcp/udp packet with source port being zero to pass through firewall.

Example

no allow-zero-Port

Syntax

ip-spoof-checking

Mode

All Modes

Description

Enable IP spoof checking.

Example

ip-spoof-checking

Syntax

no ip-spoof-checking

Mode

All Modes

Description

Disable IP spoof checking.

Example

```
no ip-spoof-checking
```

Syntax

```
port-scan-detection
```

Mode

All Modes

Description

Enable port scan detection.

Example

```
port-scan-detection
```

Syntax

```
no port-scan-detection
```

Mode

All Modes

Description

Disable port scan detection.

Example

```
no port-scan-detection
```

Syntax

```
ucapl-compliance
```

Mode

All Modes

Description

Enable UCAPL compliance.

Example

```
ucapl-compliance
```

Syntax

```
no ucapl-compliance
```

Mode

All Modes

Description

Disable UCAPL compliance.

Example

```
no ucapl-compliance
```

Syntax

```
anticipated-connection-timeout <UINT32>
```

Mode

All Modes

Description

Set timeout for anticipated TCP/UDP connections (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
anticipated-connection-timeout 10
```

Syntax

```
no anticipated-connection-timeout
```

Mode

All Modes

Description

Clear timeout for anticipated TCP/UDP connections (seconds).

Example

```
no anticipated-connection-timeout
```

Syntax

```
anticipated-connection-parent-termination
```

Mode

All Modes

Description

Enable termination of parent on timeout of anticipated TCP/UDP connections.

Example

```
anticipated-connection-parent-termination
```

Syntax

```
no anticipated-connection-parent-termination
```

Mode

All Modes

Description

Disable termination of parent on timeout of anticipated TCP/UDP connections.

Example

```
no anticipated-connection-parent-termination
```

Syntax

```
cache-ignore-icmp-reject
```

Mode

All Modes

Description

Enable don't allow ICMP TTL exceed or destination Unreachable to kill cache entries.

Example

```
cache-ignore-icmp-reject
```

Syntax

```
no cache-ignore-icmp-reject
```

Mode

All Modes

Description

Disable don't allow ICMP TTL exceed or destination Unreachable to kill cache entries.

Example

```
no cache-ignore-icmp-reject
```

Syntax

```
anticipated-media-timeout <UINT32>
```

Mode

All Modes

Description

Set timeout for anticipated media connections(seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
anticipated-media-timeout 60
```

Syntax

```
no anticipated-media-timeout
```

Mode

All Modes

Description

Clear timeout for anticipated media connections(seconds).

Example

```
no anticipated-media-timeout
```

Syntax

```
anticipated-media-parent-termination
```

Mode

All Modes

Description

Enable termination of parent on timeout of anticipated media connections.

Example

```
anticipated-media-parent-termination
```

Syntax

```
no anticipated-media-parent-termination
```

Mode

All Modes

Description

Disable termination of parent on timeout of anticipated media connections.

Example

```
no anticipated-media-parent-termination
```

Syntax

```
trace-connections-port <IPV4_PORT>
```

Mode

All Modes

Description

Set TCP port to trace connections to.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
trace-connections-port 8080
```

Syntax

no trace-connections-port

Mode

All Modes

Description

Clear TCP port to trace connections to.

Example

no trace-connections-port

Syntax

include-tcp-data-connection

Mode

All Modes

Description

Enable include TCP data connections in traces.

Example

include-tcp-data-connection

Syntax

no include-tcp-data-connection

Mode

All Modes

Description

Disable include TCP data connections in traces.

Example

no include-tcp-data-connection

Syntax

track-bandwidth-usage

Mode

All Modes

Description

Enable tracking bandwidth usage for default traffic.

Example

track-bandwidth-usage

Syntax

no track-bandwidth-usage

Mode

All Modes

Description

Disable tracking bandwidth usage for default traffic.

Example

```
no track-bandwidth-usage
```

Syntax

```
decrease-connection-count-after-close
```

Mode

All Modes

Description

Enable decreasing connection count immediately after TCP connection close.

Example

```
decrease-connection-count-after-close
```

Syntax

```
no decrease-connection-count-after-close
```

Mode

All Modes

Description

Disable decreasing connection count immediately after TCP connection close.

Example

```
no decrease-connection-count-after-close
```

Syntax

```
csrf-token-validation
```

Mode

All Modes

Description

Enable use CSRF Token Validation.

Example

```
csrf-token-validation
```

Syntax

```
no csrf-token-validation
```

Mode

All Modes

Description

Disable use CSRF Token Validation.

Example

```
no csrf-token-validation
```

Syntax

```
secure-session-id-cookie
```

Mode

All Modes

Description

Enable use secure session id cookie.

Example

```
secure-session-id-cookie
```

Syntax

```
no secure-session-id-cookie
```

Mode

All Modes

Description

Disable use secure session id cookie.

Example

```
no secure-session-id-cookie
```

Syntax

```
tcp-state-manipulation-dos-protection
```

Mode

All Modes

Description

Enable protection against TCP state manipulation DoS.

Example

```
tcp-state-manipulation-dos-protection
```

Syntax

```
no tcp-state-manipulation-dos-protection
```

Mode

All Modes

Description

Disable protection against TCP state manipulation DoS.

Example

no tcp-state-manipulation-dos-protection

Syntax

sequential-addresses

Mode

All Modes

Description

Enable allocation of sequential addresses when performing many-to-few NAT.

Example

sequential-addresses

Syntax

no sequential-addresses

Mode

All Modes

Description

Disable allocation of sequential addresses when performing many-to-few NAT.

Example

no sequential-addresses

Syntax

default-policy-editable

Mode

All Modes

Description

Enable the ability to remove and fully edit auto-added access rules and NATs.

Example

default-policy-editable

Syntax

no default-policy-editable

Mode

All Modes

Description

Disable the ability to remove and fully edit auto-added access rules and NATs.

Example

no default-policy-editable

Syntax

udp-icmp-flood-detecting

Mode

All Modes

Description

Enable aggressive UDP/ICMP flood detecting.

Example

udp-icmp-flood-detecting

Syntax

no udp-icmp-flood-detecting

Mode

All Modes

Description

Disable aggressive UDP/ICMP flood detecting.

Example

no udp-icmp-flood-detecting

Syntax

udp-icmp-flood-protection

Mode

All Modes

Description

Enable enforce UDP/ICMP flood protection with 100-millisecond resolution.

Example

udp-icmp-flood-protection

Syntax

no udp-icmp-flood-protection

Mode

All Modes

Description

Disable enforce UDP/ICMP flood protection with 100-millisecond resolution.

Example

no udp-icmp-flood-protection

Syntax

bypass-vpn-traffic

Mode

All Modes

Description

Enable bypass VPN traffic from flood protection.

Example

```
bypass-vpn-traffic
```

Syntax

```
no bypass-vpn-traffic
```

Mode

All Modes

Description

Disable bypass VPN traffic from flood protection.

Example

```
no bypass-vpn-traffic
```

Syntax

```
log-object-name
```

Mode

All Modes

Description

Enable log packet content, schedule and address object name.

Example

```
log-object-name
```

Syntax

```
no log-object-name
```

Mode

All Modes

Description

Disable log packet content, schedule and address object name.

Example

```
no log-object-name
```

Syntax

```
clear connections
```

Mode

All Modes

Description

Clear connections.

Example

```
flush connections
```

Syntax

```
reset-login-counter <UINT32>
```

Mode

All Modes

Description

Reset user succesful login counter (hours).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
reset-login-counter 100
```

Syntax

```
no reset-login-counter
```

Mode

All Modes

Description

Clear reset user succesful login counter.

Example

```
no reset-login-counter
```

Syntax

```
send-rst-on-timeout
```

Mode

All Modes

Description

Enable send RST on timeout TCP connection.

Example

```
send-rst-on-timeout
```

Syntax

```
no send-rst-on-timeout
```

Mode

All Modes

Description

Disable send RST on timeout TCP connection.

Example

```
no send-rst-on-timeout
```

Syntax

```
async-save-flash-period <UINT16>
```

Mode

All Modes

Description

Set the async save flash period in seconds (Note: any changes during the period may loss if unexpected power outage).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
async-save-flash-period 60
```

Syntax

```
diag advanced security-services
```

Mode

Config

Description

Configure advanced diag security services settings.

Example

```
diag advanced security-services
```

Syntax

```
dpi-engine
```

Mode

Diag Advanced Security Services Settings

Description

Enable DPI engine.

Example

```
dpi-engine
```

Syntax

```
no dpi-engine
```

Mode

Diag Advanced Security Services Settings

Description

Disable DPI engine.

Example

```
no dpi-engine
```

Syntax

```
bidirectional-ips
```

Mode

Diag Advanced Security Services Settings

Description

Enable applying IPS signatures bidirectionally.

Example

```
bidirectional-ips
```

Syntax

```
no bidirectional-ips
```

Mode

Diag Advanced Security Services Settings

Description

Disable applying IPS signatures bidirectionally.

Example

```
no bidirectional-ips
```

Syntax

```
dpi-ip-fragment-reassembly
```

Mode

Diag Advanced Security Services Settings

Description

Enable IP fragment reassembly in DPI.

Example

```
dpi-ip-fragment-reassembly
```

Syntax

```
no dpi-ip-fragment-reassembly
```

Mode

Diag Advanced Security Services Settings

Description

Disable IP fragment reassembly in DPI.

Example

```
no dpi-ip-fragment-reassembly
```

Syntax

```
dev-debug
```

Mode

Diag Advanced Security Services Settings

Description

Enable extra dev debug info.

Example

```
dev-debug
```

Syntax

```
no dev-debug
```

Mode

Diag Advanced Security Services Settings

Description

Disable extra dev debug info.

Example

```
no dev-debug
```

Syntax

```
tcp-sequence-adjustment
```

Mode

Diag Advanced Security Services Settings

Description

Enable TCP expected sequence adjustment in DPI.

Example

```
tcp-sequence-adjustment
```

Syntax

```
no tcp-sequence-adjustment
```

Mode

Diag Advanced Security Services Settings

Description

Disable TCP expected sequence adjustment in DPI.

Example

no tcp-sequence-adjustment

Syntax

proxy-email-packets

Mode

Diag Advanced Security Services Settings

Description

Enable proxy email packets in DPI.

Example

proxy-email-packets

Syntax

no proxy-email-packets

Mode

Diag Advanced Security Services Settings

Description

Disable proxy email packets in DPI.

Example

no proxy-email-packets

Syntax

smtp-chunking-modification

Mode

Diag Advanced Security Services Settings

Description

Enable App-Firewall SMTP CHUNKING modification.

Example

smtp-chunking-modification

Syntax

no smtp-chunking-modification

Mode

Diag Advanced Security Services Settings

Description

Disable App-Firewall SMTP CHUNKING modification.

Example

no smtp-chunking-modification

Syntax

pop3-auto-deletion

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV POP3 auto deletion.

Example

pop3-auto-deletion

Syntax

no pop3-auto-deletion

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV POP3 auto deletion.

Example

no pop3-auto-deletion

Syntax

pop3-uidl-rewriting

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV POP3 UIDL rewriting.

Example

pop3-uidl-rewriting

Syntax

no pop3-uidl-rewriting

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV POP3 UIDL rewriting.

Example

no pop3-uidl-rewriting

Syntax

smb-read-write-enforcement

Mode

Diag Advanced Security Services Settings

Description

Enable gateway AV SMB read/write ordering enforcement.

Example

smb-read-write-enforcement

Syntax

no smb-read-write-enforcement

Mode

Diag Advanced Security Services Settings

Description

Disable gateway AV SMB read/write ordering enforcement.

Example

no smb-read-write-enforcement

Syntax

keep-http-accept-range-bytes

Mode

Diag Advanced Security Services Settings

Description

Keep HTTP header Accept-range: bytes.

Example

keep-http-accept-range-bytes

Syntax

no keep-http-accept-range-bytes

Mode

Diag Advanced Security Services Settings

Description

Don't keep HTTP header Accept-range: bytes.

Example

no keep-http-accept-range-bytes

Syntax

log-virus-uri

Mode

Diag Advanced Security Services Settings

Description

Enable log virus URI.

Example

```
log-virus-uri
```

Syntax

```
no log-virus-uri
```

Mode

Diag Advanced Security Services Settings

Description

Disable log virus URI.

Example

```
no log_virus_uri
```

Syntax

```
offset-qualifier-signature
```

Mode

Diag Advanced Security Services Settings

Description

Enable apply signatures containing file offset qualifiers
 that trigger on TCP streams with unidentified protocols.

Example

```
offset-qualifier-signature
```

Syntax

```
no offset-qualifier-signature
```

Mode

Diag Advanced Security Services Settings

Description

Disable apply signatures containing file offset qualifiers
 that trigger on TCP streams with unidentified protocols.

Example

```
no offset-qualifier-signature
```

Syntax

```
minimum-http-header-length <UINT16>
```

Mode

Diag Advanced Security Services Settings

Description

Set minimum HTTP header length (0 to disable).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
minimum-http-header-length 0
```

Syntax

```
no minimum-http-header-length
```

Mode

Diag Advanced Security Services Settings

Description

Clear minimum HTTP header length (0 to disable).

Example

```
no minimum-http-header-length
```

Syntax

```
incremental-signature-updates
```

Mode

Diag Advanced Security Services Settings

Description

Enable incremental updates to IDP, GAV and SPY signature databases.

Example

```
incremental-signature-updates
```

Syntax

```
no incremental-signature-updates
```

Mode

Diag Advanced Security Services Settings

Description

Disable incremental updates to IDP, GAV and SPY signature databases.

Example

```
no incremental-signature-updates
```

Syntax

```
handle-http2
```

Mode

Diag Advanced Security Services Settings

Description

Enable handle HTTP/2.

Example

```
handle-http2
```

Syntax

```
no handle-http2
```

Mode

Diag Advanced Security Services Settings

Description

Disable handle HTTP/2.

Example

```
no handle-http2
```

Syntax

```
force-utm-offload
```

Mode

Diag Advanced Security Services Settings

Description

Enable force UTM offload.

Example

```
force-utm-offload
```

Syntax

```
no force-utm-offload
```

Mode

Diag Advanced Security Services Settings

Description

Disable force UTM offload.

Example

```
no force-utm-offload
```

Syntax

```
utm-traffic-offload <UINT8>
```

Mode

Diag Advanced Security Services Settings

Description

Set Active/Active UTM traffic Offload percentage.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
utm-traffic-offload 60
```

Syntax

```
no utm-traffic-offload
```

Mode

Diag Advanced Security Services Settings

Description

Clear Active/Active UTM traffic Offload percentage.

Example

```
no utm-traffic-offload
```

Syntax

```
limit-dpi-tcp-window-advertisement [ maximum <UINT16> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable enforcement of a limit on maximum allowed advertised TCP window with any DPI-based service enabled and set the maximum allowed.

Options

maximum Set the maximum allowed advertised TCP window with any DPI-based service enabled.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
limit-dpi-tcp-window-advertisement maximum 256
```

Syntax

```
no limit-dpi-tcp-window-advertisement
```

Mode

Diag Advanced Security Services Settings

Description

Disable enforcement of a limit on maximum allowed advertised TCP window with any DPI-based service enabled.

Example

```
no limit-dpi-tcp-window-advertisement
```

Syntax

```
threshold-limit <UINT32>
```

Mode

Diag Advanced Security Services Settings

Description

Threshold above which size limits are enforced on regex automaton.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
threshold-limit 5000
```

Syntax

```
maximum-regex-automaton-size <UINT32>
```

Mode

Diag Advanced Security Services Settings

Description

Maximum allowed size for regex automaton.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
maximum-regex-automaton-size 10000
```

Syntax

```
signature-database-reload
```

Mode

Diag Advanced Security Services Settings

Description

Enable signature database reload.

Example

```
signature-database-reload
```

Syntax

```
no signature-database-reload
```

Mode

Diag Advanced Security Services Settings

Description

Disable signature database reload.

Example

no signature-database-reload

Syntax

process-ips-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of IPS signatures.

Example

process-ips-signatures

Syntax

no process-ips-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of IPS signatures.

Example

no process-ips-signatures

Syntax

process-gav-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of GAV signatures.

Example

process-gav-signatures

Syntax

no process-gav-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of GAV signatures.

Example

no process-gav-signatures

Syntax

process-anti-spyware-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of Anti-Spyware signatures.

Example

process-anti-spyware-signatures

Syntax

no process-anti-spyware-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of Anti-Spyware signatures.

Example

no process-anti-spyware-signatures

Syntax

process-app-signatures

Mode

Diag Advanced Security Services Settings

Description

Enable processing of App signatures.

Example

process-app-signatures

Syntax

no process-app-signatures

Mode

Diag Advanced Security Services Settings

Description

Disable processing of App signatures.

Example

no process-app-signatures

Syntax

optimal-value [val <UINT32>]

Mode

Diag Advanced Security Services Settings

Description

Enable optimal value and set the value.

Options

- val*** Set the optimal value.
- <UINT32>*** Integer in the form: D OR 0xHHHHHHHH. Example: *123*

Example

optimal-value 10240

Syntax

no optimal-value

Mode

Diag Advanced Security Services Settings

Description

Disable optimal value and set the value.

Example

no optimal-value

Syntax

limit-ips-cft-scan

Mode

Diag Advanced Security Services Settings

Description

Eable limit IPS CFT scan.

Example

limit-ips-cft-scan

Syntax

no limit-ips-cft-scan

Mode

Diag Advanced Security Services Settings

Description

Disable limit IPS CFT scan.

Example

no limit-ips-cft-scan

Syntax

```
enforce-cfs-host-tag-search
```

Mode

Diag Advanced Security Services Settings

Description

Enable enforcement of host tag search for CFS.

Example

```
enforce-cfs-host-tag-search
```

Syntax

```
no enforce-cfs-host-tag-search
```

Mode

Diag Advanced Security Services Settings

Description

Disable enforcement of host tag search for CFS.

Example

```
no enforce-cfs-host-tag-search
```

Syntax

```
local-cfs-server [ primary <HOSTNAME_MIXED> ] [ secondary <HOSTNAME_MIXED> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable local CFS server and set the IP addresses.

Options

primary	Primary local CFS server.
<HOSTNAME_MIXED>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: 2001:cdba:0000:0000:0000:0000:3257:9652\n
secondary	Secondary local CFS server.
<HOSTNAME_MIXED>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
local-cfs-server
local-cfs-server primary 10.10.10.10
local-cfs-server secondary 10.10.10.11
```

Syntax

```
no local-cfs-server
```

Mode

Diag Advanced Security Services Settings

Description

Disable local CFS server.

Example

```
no local-cfs-server
```

Syntax

```
reset licenses
```

Mode

Diag Advanced Security Services Settings

Description

Reset licenses and security services info.

Example

```
reset licenses
```

Syntax

```
reset http-clientless-notification-cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset HTTP clientless notification cache.

Example

```
reset http-clientless-notification-cache
```

Syntax

```
reset cloud-av-cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset cloud AV cache.

Example

```
reset cloud-av-cache
```

Syntax

```
cloud-av-server [ host <HOSTNAME> ]
```

Mode

Diag Advanced Security Services Settings

Description

Enable private cloud AV server and set the IP address.

Options

host	Private cloud AV server IP or name.

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
cloud-av-server
cloud-av-server host 10.10.10.12
```

Syntax

```
no cloud-av-server
```

Mode

Diag Advanced Security Services Settings

Description

Disable private cloud AV server.

Example

```
no cloud-av-server
```

Syntax

```
reset cfs-memory-cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset cfs memory cache.

Example

```
reset cfs memory cache
```

Syntax

```
reset cfs-persistent-cache
```

Mode

Diag Advanced Security Services Settings

Description

Reset cfs persistent cache.

Example

```
reset cfs persistent cache
```

Syntax

```
reset client-enforcement-status-info
```

Mode

Diag Advanced Security Services Settings

Description

Reset client enforcement status info.

Example

```
reset client-enforcement-status-info
```

Syntax

```
reset registration-log
```

Mode

Diag Advanced Security Services Settings

Description

reset registartion log.

Example

```
reset registration-log
```

Syntax

```
diag advanced dpi-ssl
```

Mode

Config

Description

Configure advanced diag DPI-SSL settings.

Example

```
diag advanced dpi-ssl
```

Syntax

```
rewritten-certificate-sn-modifier <UINT16>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set rewritten certificate SN modifier.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
rewritten-certificate-sn-modifier 1
```

Syntax

```
client-spoofed-certificate-caching
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable client spoofed certificate caching.

Example

```
client-spoofed-certificate-caching
```

Syntax

```
no client-spoofed-certificate-caching
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable client spoofed certificate caching.

Example

```
no client-spoofed-certificate-caching
```

Syntax

```
remove-tcp-timestamp-option
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable removing TCP timestamp option.

Example

```
remove-tcp-timestamp-option
```

Syntax

```
no remove-tcp-timestamp-option
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable removing TCP timestamp option.

Example

```
no remove-tcp-timestamp-option
```

Syntax

```
drop-ssl-on-low-memory
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable dropping SSL packets when memory low.

Example

drop-ssl-on-low-memory

Syntax

no drop-ssl-on-low-memory

Mode

Diag Advanced DPI-SSL Settings

Description

Disable dropping SSL packets when memory low.

Example

no drop-ssl-on-low-memory

Syntax

proxyless-ssl-when-limit-exceeded

Mode

Diag Advanced DPI-SSL Settings

Description

Enable allowing SSL without proxy when connection limit exceeded.

Example

proxyless-ssl-when-limit-exceeded

Syntax

no proxyless-ssl-when-limit-exceeded

Mode

Diag Advanced DPI-SSL Settings

Description

Disable allowing SSL without proxy when connection limit exceeded.

Example

no proxyless-ssl-when-limit-exceeded

Syntax

endpoint-tcp-window-setup

Mode

Diag Advanced DPI-SSL Settings

Description

Enable endpoint TCP window setup.

Example

endpoint-tcp-window-setup

Syntax

no endpoint-tcp-window-setup

Mode

Diag Advanced DPI-SSL Settings

Description

Disable endpoint TCP window setup.

Example

no endpoint-tcp-window-setup

Syntax

server-facing-session-reuse

Mode

Diag Advanced DPI-SSL Settings

Description

Enable server facing cache.

Example

server-facing-session-reuse

Syntax

no server-facing-session-reuse

Mode

Diag Advanced DPI-SSL Settings

Description

Disable server facing cache.

Example

no server-facing-session-reuse

Syntax

client-facing-session-reuse

Mode

Diag Advanced DPI-SSL Settings

Description

Enable client facing cache.

Example

client-facing-session-reuse

Syntax

no client-facing-session-reuse

Mode

Diag Advanced DPI-SSL Settings

Description

Disable client facing cache.

Example

```
no client-facing-session-reuse
```

Syntax

```
ip-based-exclusion-cache
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable IP based exclusion cache.

Example

```
ip-based-exclusion-cache
```

Syntax

```
no ip-based-exclusion-cache
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable IP based exclusion cache.

Example

```
no ip-based-exclusion-cache
```

Syntax

```
use-2048-bit-certificate-key
```

Mode

Diag Advanced DPI-SSL Settings

Description

Use 2048 bit spoof certificate key in DPI SSL.

Example

```
use-2048-bit-certificate-key
```

Syntax

```
no use-2048-bit-certificate-key
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable use 2048 bit spoof certificate key in DPI SSL.

Example

```
no use-2048-bit-certificate-key
```

Syntax

```
dynamic-exclusion-for-excluded-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable Dynamic Exclusion for exclude connections.

Example

```
dynamic-exclusion-for-excluded-connections
```

Syntax

```
no dynamic-exclusion-for-excluded-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable dynamic exclusion for excluded connections.

Example

```
no dynamic-exclusion-for-excluded-connections
```

Syntax

```
connection-failures max-supported-entries <UINT32>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Maximum entries for connection failures.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
connection-failures max-supported-entries 100
```

Syntax

```
connection-failures max-similar-failures <UINT32>
```

Mode

Description

Maximum similar failures.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
connection-failures max-similar-failures 20
```

Syntax

```
connection-failures rollover-failed-entries
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable rollover failed entries for connection failures.

Example

```
connection-failures rollover-failed-entries
```

Syntax

```
no connection-failures rollover-failed-entries
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable rollover failed entries for connection failures.

Example

```
no connection-failures rollover-failed-entries
```

Syntax

```
revocation-check-server-certificate
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable check for server certificate revocation.

Example

```
revocation-check-server-certificate
```

Syntax

```
no revocation-check-server-certificate
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable check for server certificate revocation.

Example

```
no revocation-check-server-certificate
```

Syntax

```
expired-certificate-authority
```

Mode

Diag Advanced DPI-SSL Settings

Description

Allow Expired certificate authority.

Example

```
expired-certificate-authority
```

Syntax

```
no expired-certificate-authority
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable expired certificate authority.

Example

```
no expired-certificate-authority
```

Syntax

```
block-untrusted-certificate-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Enable blocking connections to sites with untrusted certificates.

Example

```
block-untrusted-certificate-connections
```

Syntax

```
no block-untrusted-certificate-connections
```

Mode

Diag Advanced DPI-SSL Settings

Description

Disable blocking connections to sites with untrusted certificates.

Example

```
no block-untrusted-certificate-connections
```

Syntax

```
max-stream-offset <UINT16>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set max stream offset to check for SSL client-hello resemblance.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
max-stream-offset 512
```

Syntax

```
no max-stream-offset
```

Mode

Diag Advanced DPI-SSL Settings

Description

Clear max stream offset to check for SSL client-hello resemblance.

Example

```
no max-stream-offset
```

Syntax

```
tcp-window-multiplier <UINT8>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set TCP window multiplier (N *64k).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tcp-window-multiplier 8
```

Syntax

```
tcp-min-adv-window <UINT8>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set TCP Min Advertised window (N * 1k).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tcp-min-adv-window 16
```

Syntax

```
tcp-duplicate-ack-response-threshold <UINT16>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set TCP Duplicate Ack response threshold.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
tcp-duplicate-ack-response-threshold 1024
```

Syntax

```
extended-memory-implementation <UINT8>
```

Mode

Diag Advanced DPI-SSL Settings

Description

Settings for Extended Memory Implementation.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
extended-memory-implementation 2
```

Syntax

```
max-proxied-connections <UINT16>
```

Mode

Description

Set the override for max proxied SSL connections.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

max-proxied-connections 0

Syntax

no max-proxied-connections

Mode

Diag Advanced DPI-SSL Settings

Description

Clear the override for max proxied SSL connections.

Example

no max-proxied-connections

Syntax

update-security-services-info

Mode

Diag Advanced DPI-SSL Settings

Description

Update licenses and security services info.

Example

update-security-services-info

Syntax

clear internal-session-and-cache-state

Mode

Diag Advanced DPI-SSL Settings

Description

Clear internal session and cache state for debug.

Example

clear internal-session-and-cache-state

Syntax

ssl-version { all | ssl-v3 | tls-v10 | tls-v11 | tls-v12 | tls-v13 }

Mode

Diag Advanced DPI-SSL Settings

Description

Set ssl version.

Options

all All versions.

ssl-v3 ssl version3.0.

tls-v10 tls version1.0.

tls-v11 tls version1.1.

tls-v12 tls version1.2.

tls-v13 tls version1.3.

Example

```
ssl-version ssl-v3
```

Syntax

```
cipher-method { compatible | secure }
```

Mode

Diag Advanced DPI-SSL Settings

Description

Set ssl cipher method.

Options

compatible Compatible ciphers method.

secure Secure ciphers method.

Example

```
cipher-method secure
```

Syntax

```
diag advanced high-availability
```

Mode

Config

Description

Configure advanced diag High Availability settings.

Example

```
diag advanced high-availability
```

Syntax

idle-monitor

Mode

Diag Advanced High Availability Settings

Description

Enable network monitor probing on idle unit.

Example

idle-monitor

Syntax

no idle-monitor

Mode

Diag Advanced High Availability Settings

Description

Disable network monitor probing on idle unit.

Example

no idle-monitor

Syntax

suppress-active-transition-alarm

Mode

Diag Advanced High Availability Settings

Description

Enable suppressing alarm on HA transition to active.

Example

suppress-active-transition-alarm

Syntax

no suppress-active-transition-alarm

Mode

Diag Advanced High Availability Settings

Description

Disable suppressing alarm on HA transition to active.

Example

no suppress-active-transition-alarm

Syntax

multi-chassis-lag

Mode

Diag Advanced High Availability Settings

Description

Enable support for multi chassis LAG on Active/Standby noth units.

Example

```
multi-chassis-lag
```

Syntax

```
no multi-chassis-lag
```

Mode

Diag Advanced High Availability Settings

Description

Disable support for multi chassis LAG on Active/Standby noth units.

Example

```
no multi-chassis-lag
```

Syntax

```
restart-backup-on-watchdog
```

Mode

Diag Advanced High Availability Settings

Description

Enable always restarting HA backup for watchdog task.

Example

```
restart-backup-on-watchdog
```

Syntax

```
no restart-backup-on-watchdog
```

Mode

Diag Advanced High Availability Settings

Description

Disable always restarting HA backup for watchdog task .

Example

```
no restart-backup-on-watchdog
```

Syntax

```
interleave-cache
```

Mode

Diag Advanced High Availability Settings

Description

Enable interleave connection cache state synchronization messages.

Example

```
interleave-cache
```

Syntax

```
no interleave-cache
```

Mode

Diag Advanced High Availability Settings

Description

Disable interleave connection cache state synchronization messages.

Example

```
no interleave-cache
```

Syntax

```
transparent-mode-gratuitous-arp
```

Mode

Diag Advanced High Availability Settings

Description

Enable sending gratuitous ARP to DMZ or LAN on transparent mode while HA failover.

Example

```
transparent-mode-gratuitous-arp
```

Syntax

```
no transparent-mode-gratuitous-arp
```

Mode

Diag Advanced High Availability Settings

Description

Disable sending gratuitous ARP to DMZ or LAN on transparent mode while HA failover.

Example

```
no transparent-mode-gratuitous-arp
```

Syntax

```
max-transparent-mode-gratuitous-arps <UINT32>
```

Mode

Diag Advanced High Availability Settings

Description

Set maximum number of gratuitous ARP of transparent mode per interface while HA failover.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
max-transparent-mode-gratuitous-arps 256
```

Syntax

```
max-gratuitous-arps <UINT32>
```

Mode

Diag Advanced High Availability Settings

Description

Set maximum number of gratuitous ARP while HA failover.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
max-gratuitous-arps 1
```

Syntax

```
diag advanced pppoe
```

Mode

Config

Description

Configure advanced diag PPPoE settings.

Example

```
diag advanced pppoe
```

Syntax

```
lcp-requests
```

Mode

Diag Advanced PPPoE Settings

Description

Enable allowing LCP requests to PPPoE server.

Example

```
lcp-requests
```

Syntax

```
no lcp-requests
```

Mode

Diag Advanced PPPoE Settings

Description

Disable allowing LCP requests to PPPoE server.

Example

```
no lcp-requests
```

Syntax

```
log-lcp-echo
```

Mode

Diag Advanced PPPoE Settings

Description

Enable logging LCP echo requests and replies between client and server.

Example

```
log-lcp-echo
```

Syntax

```
no log-lcp-echo
```

Mode

Diag Advanced PPPoE Settings

Description

Disable logging LCP echo requests and replies between client and server.

Example

```
no log-lcp-echo
```

Syntax

```
end-of-list-tag
```

Mode

Diag Advanced PPPoE Settings

Description

Enable PPPoE End-Of-List tag.

Example

```
end-of-list-tag
```

Syntax

```
no end-of-list-tag
```

Mode

Diag Advanced PPPoE Settings

Description

Disable PPPoE End-Of-List tag.

Example

```
no end-of-list-tag
```

Syntax

```
netmask <HOST_IP>
```

Mode

Diag Advanced PPPoE Settings

Description

Set PPPoE netmask.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
netmask 255.255.255.252
```

Syntax

```
no netmask
```

Mode

Diag Advanced PPPoE Settings

Description

Clear PPPoE netmask.

Example

```
no netmask
```

Syntax

```
diag advanced dial-up
```

Mode

Config

Description

Configure advanced diag dial-up settings.

Example

```
diag advanced dial-up
```

Syntax

```
max-pppdu-failure <UINT16>
```

Mode

Diag Advanced Dial-Up Settings

Description

Set PPPDU max configuration failure number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-pppdu-failure 9
```

Syntax

```
reset
```

Mode

Diag Advanced Dial-Up Settings

Description

Restart dial-up devices.

Example

```
reset
```

Syntax

```
diag advanced dpi-stateful-firewall-security
```

Mode

Config

Description

DPI and stateful firewall security.

Example

```
diag advanced dpi-stateful-firewall-security
```

Syntax

```
diag advanced stateful-firewall-security
```

Mode

Config

Description

Stateful firewall security.

Example

```
diag advanced stateful-firewall-security
```

Syntax

```
diag advanced management
```

Mode

Config

Description

Configure advanced diag management settings.

Example

```
diag advanced management
```

Syntax

```
sonicui7-as-default
```

Mode

Diag Advanced Management Settings

Description

Enable SonicUI7 as default management GUI.

Example

```
sonicui7-as-default
```

Syntax

```
no sonicui7-as-default
```

Mode

Diag Advanced Management Settings

Description

Disable SonicUI7 as default management GUI.

Example

```
no sonicui7-as-default
```

Syntax

```
new-license-page-format
```

Mode

Diag Advanced Management Settings

Description

Enable use new license page format.

Example

```
new-license-page-format
```

Syntax

```
no new-license-page-format
```

Mode

Diag Advanced Management Settings

Description

Disable use new license page format.

Example

```
no new-license-page-format
```

Syntax

```
standby-management-sa
```

Mode

Diag Advanced Management Settings

Description

Enable using standby management SA.

Example

```
standby-management-sa
```

Syntax

```
no standby-management-sa
```

Mode

Diag Advanced Management Settings

Description

Disable using standby management SA.

Example

```
no standby-management-sa
```

Syntax

```
gms-preempts-admin
```

Mode

Diag Advanced Management Settings

Description

Enable allowing SGMS to preempt a logged in administrator.

Example

```
gms-preempts-admin
```

Syntax

```
no gms-preempts-admin
```

Mode

Diag Advanced Management Settings

Description

Disable allowing SGMS to preempt a logged in administrator.

Example

```
no gms-preempts-admin
```

Syntax

```
http-management
```

Mode

Diag Advanced Management Settings

Description

Allow management via HTTP.

Example

```
http-management
```

Syntax

```
no http-management
```

Mode

Diag Advanced Management Settings

Description

Disable allow management via HTTP.

Example

```
no http-management
```

Syntax

```
classic-view
```

Mode

Diag Advanced Management Settings

Description

Show classic address Objects, services and NAT policies view pages.

Example

```
classic-view
```

Syntax

```
no classic-view
```

Mode

Diag Advanced Management Settings

Description

Disable show classic address objects, services and NAT policies view pages.

Example

```
no classic-view
```

Syntax

```
online-help-url { default | override [ url <WORD> ] }
```

Mode

Diag Advanced Management Settings

Description

Set the online help URL.

Options

default	Use the default global help system URL.
override	Override the default using the configured value.
url	Set URL.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
online-help-url url "help.mysonicwall.com/help.asp"
```

Syntax

```
diag advanced user-authentication
```

Mode

Config

Description

Configure advanced diag user authentication settings.

Example

```
diag advanced user-authentication
```

Syntax

```
post-authentication-redirect-url <URL>
```

Mode

Diag Advanced User Authentication Settings

Description

Set post authentication user redirect URL.

Options

<URL>	URL in the form: http://host/file. Example: <i>http://www.example.com/products/</i>

Example

```
post-authentication-redirect-url "10.10.10.10/welcome.asp"
```

Syntax

no post-authentication-redirect-url

Mode

Diag Advanced User Authentication Settings

Description

Clear post authentication user redirect URL.

Example

no post-authentication-redirect-url

Syntax

redirect-https

Mode

Diag Advanced User Authentication Settings

Description

Enable redirecting unauthenticated HTTPS connections to the login page.

Example

redirect-https

Syntax

no redirect-https

Mode

Diag Advanced User Authentication Settings

Description

Disable redirecting unauthenticated HTTPS connections to the login page.

Example

no redirect-https

Syntax

https-redirect-port <UINT32>

Mode

Diag Advanced User Authentication Settings

Description

Set the internal NAT TCP port number for HTTPS redirect.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

https-redirect-port 3443

Syntax

flush-cached-redirect-files

Mode

Diag Advanced User Authentication Settings

Description

Flush all files (redirect pages etc.) cached for redirecting.

Example

flush-cached-redirect-files

Syntax

logout users

Mode

Diag Advanced User Authentication Settings
Top Level
Config

Description

Logout all users.

Example

logout users

Syntax

kill inactive-users { all | ntlm | rad-acct | sso-agent | tsa }

Mode

Diag Advanced User Authentication Settings
Top Level
Config

Description

kill all inactive users.

Options

- all*** Kill all inactive users indentified by all type of users.
- ntlm*** Kill all inactive users identified by ntlm
- rad-acct*** Kill all inactive users identified by radius accounting
- sso-agent*** Kill all inactive users identified by sso-agent.
- tsa*** Kill all inactive users identified by tsa.

Example

kill inactive-users

Syntax

log-all-sso-attempts { enable | event-log | sso-auth-log }

Mode

Diag Advanced User Authentication Settings

Description

Enable logging an audit trail of all SSO attempts in the event log.

Options

<i>enable</i>	Enable logging an audit trail of all SSO attempts in the event log.
<i>event-log</i>	Log in the event log.
<i>sso-auth-log</i>	Log in /data/sonicwall/sonicos/logs/ssoauth.log.

Example

log-all-sso-attempts enable

Syntax

no log-all-sso-attempts enable

Mode

Diag Advanced User Authentication Settings

Description

Disable logging an audit trail of all SSO attempts in the event log.

Options

<i>enable</i>	Enable logging an audit trail of all SSO attempts in the event log.

Example

no log-all-sso-attempts

Syntax

user-ip { all | group <ADDR_GROUP_NAME> | name <ADDR_NAME> }

Mode

Diag Advanced User Authentication Settings

Description

Set user ip address object name or group name.

Options

<i>all</i>	All.
<i>group</i>	Address group name.
<i><ADDR_GROUP_NAME></i>	Group address object name. Example: <i>Sales Group</i>
<i>name</i>	Address object name.
<i><ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>

Example

user-ip group "ALL X1 Managemetn IP"

Syntax

include-sso-polling

Mode

Diag Advanced User Authentication Settings

Description

Enable inclusion of polling events in the SSO audit trail log.

Example

include-sso-polling

Syntax

no include-sso-polling

Mode

Diag Advanced User Authentication Settings

Description

Disable inclusion of polling events in the SSO audit trail log.

Example

no include-sso-polling

Syntax

include-sso-bypass

Mode

Diag Advanced User Authentication Settings

Description

Enable inclusion of SSO bypass events in the SSO audit trail log.

Example

include-sso-bypass

Syntax

no include-sso-bypass

Mode

Diag Advanced User Authentication Settings

Description

Disable inclusion of SSO bypass events in the SSO audit trail log.

Example

no include-sso-bypass

Syntax
<i>include-additional-non-initiation</i>
Mode
Diag Advanced User Authentication Settings
Description
Enable inclusion of additional non-initiation of SSO in the SSO audit trail log.
Example
<i>include-additional-non-initiation</i>

Syntax
<i>no include-additional-non-initiation</i>
Mode
Diag Advanced User Authentication Settings
Description
Disable inclusion of additional non-initiation of SSO in the SSO audit trail log.
Example
<i>no include-additional-non-initiation</i>

Syntax
<i>sso-agent-version-negotiation <UINT32></i>
Mode
Diag Advanced User Authentication Settings
Description
Set version try to negotiate SSO agent protocol to(default version 5).
Options
<UINT32> Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
Example
<i>sso-agent-version-negotiation 5</i>

Syntax
<i>no sso-agent-version-negotiation</i>
Mode
Diag Advanced User Authentication Settings
Description
Disable to negotiate SSO agent protocol version.
Example
<i>no sso-agent-version-negotiation</i>

Syntax

diag advanced diagnostics

Mode

Config

Description

Configure advanced diag diagnostics settings.

Example

diag advanced diagnostics

Syntax

setup-tool-server

Mode

Diag Advanced Diagnostics Settings

Description

Enable SonicSetup/Setuptools server.

Example

setup-tool-server

Syntax

no setup-tool-server

Mode

Diag Advanced Diagnostics Settings

Description

Disable SonicSetup/Setuptools server.

Example

no setup-tool-server

Syntax

trace-message-level { error | fatal | info | verbose | warning }

Mode

Diag Advanced Diagnostics Settings

Description

Set the trace message level.

Options

error Error.

fatal Fatal.

info Info.

verbose Verbose.

warning Warning.

Example

```
trace-message-level
```

Syntax

```
auto-restart [ every <UINT32> ]
```

Mode

Diag Advanced Diagnostics Settings

Description

Enable (for diagnostic testing purposes) auto-restarting system every set amount of minutes.

Options

every Set number of minutes to auto-restart system.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
auto-restart every 60
```

Syntax

```
no auto-restart
```

Mode

Diag Advanced Diagnostics Settings

Description

Disable (for diagnostic testing purposes) auto-restarting system every set amount of minutes.

Example

```
no auto-restart
```

Syntax

```
secured-crash-analysis
```

Mode

Diag Advanced Diagnostics Settings

Description

Enable secured www.mysonicwall.com crash analysis.

Example

```
secured-crash-analysis
```

Syntax

```
no secured-crash-analysis
```

Mode

Diag Advanced Diagnostics Settings

Description

Disable secured www.mysonicwall.com crash analysis.

Example

```
no secured-crash-analysis
```

Syntax

```
show-user-diagnostics
```

Mode

Diag Advanced Diagnostics Settings

Description

Enable to show user diagnostics on web block by CFS.

Example

```
show-user-diagnostics
```

Syntax

```
no show-user-diagnostics
```

Mode

Diag Advanced Diagnostics Settings

Description

Disable to show user diagnostics on web block by CFS.

Example

```
no show-user-diagnostics
```

Syntax

```
wan-connectivity-test start
```

Mode

Diag Advanced Diagnostics Settings

Description

WAN connectivity test.

Example

```
wan-connectivity-test start
```

Syntax

```
wan-connectivity-test target-ip <IPV4_HOST>
```

Mode

Diag Advanced Diagnostics Settings

Description

Set WAN connectivity test target IP.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wan-connectivity-test target-ip 10.10.10.10
```

Syntax

```
no wan-connectivity-test target-ip
```

Mode

Diag Advanced Diagnostics Settings

Description

Clear WAN connectivity test target IP.

Example

```
no wan-connectivity target-ip
```

Syntax

```
wan-connectivity-test stop
```

Mode

Diag Advanced Diagnostics Settings

Description

WAN connectivity test.

Example

```
wan-connectivity-test stop
```

Syntax

```
send wan-connectivity-test log
```

Mode

Diag Advanced Diagnostics Settings

Description

Send WAN connectivity state log.

Example

```
send wan-connectivity-test log
```

Syntax

```
dp-jobs-tracked <UINT8>
```

Mode

Description

Set number of jobs executed by data plane task to be tracked.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

dp-jobs-tracked 10

Syntax

suspend-assert-failure-task

Mode

Diag Advanced Diagnostics Settings

Description

Suspend the task on assert failure (debug firmware only).

Example

suspend-assert-failure-task

Syntax

no suspend-assert-failure-task

Mode

Diag Advanced Diagnostics Settings

Description

Disable suspend the task on assert failure (debug firmware only).

Example

no suspend-assert-failure-task

Syntax

check-potential-deadlocks { network-io | taking-semaphore }

Mode

Diag Advanced Diagnostics Settings

Description

Check for potential semaphore deadlocks in network I/O or when taking semaphore (debug firmware only).

Options

network-io network I/O.

taking-semaphore When taking semaphore.

Example

check-potential-deadlocks network-io

Syntax

```
no check-potential-deadlocks { network-io | taking-semaphore }
```

Mode

Diag Advanced Diagnostics Settings

Description

Disable to check for potential semaphore deadlocks in network I/O or when taking semaphore (debug firmware only).

Options

network-io network I/O.

taking-semaphore When taking semaphore.

Example

```
no check-semaphore-deadlocks network-io
```

Syntax

```
diag advanced watchdog
```

Mode

Config

Description

Configure advanced diag watchdog settings.

Example

```
diag advanced watchdog
```

Syntax

```
cpu-watchdog
```

Mode

Diag Advanced Watchdog Settings

Description

Enable CPU watchdog.

Example

```
cpu-watchdog
```

Syntax

```
no cpu-watchdog
```

Mode

Diag Advanced Watchdog Settings

Description

Disable CPU watchdog.

Example

```
no cpu-watchdog
```

Syntax

```
restart-for
```

Mode

Diag Advanced Watchdog Settings

Description

Enable restarting for watchdog task.

Example

```
restart-for
```

Syntax

```
no restart-for
```

Mode

Diag Advanced Watchdog Settings

Description

Disable restarting for watchdog task.

Example

```
no restart-for
```

Syntax

```
quick-restart
```

Mode

Diag Advanced Watchdog Settings

Description

Enable restarting quickly after an exception.

Example

```
quick-restart
```

Syntax

```
no quick-restart
```

Mode

Diag Advanced Watchdog Settings

Description

Disable restarting quickly after an exception.

Example

no quick-restart

Syntax

restart-when-no-packet-rx

Mode

Diag Advanced Watchdog Settings

Description

Enable rstart when no packet Rx activity is detected.

Example

restart-when-no-packet-rx

Syntax

no restart-when-no-packet-rx

Mode

Diag Advanced Watchdog Settings

Description

Disable rstart when no packet Rx activity is detected.

Example

no restart-when-no-packet-rx

Syntax

wait-for-no-packet-rx <UINT16>

Mode

Diag Advanced Watchdog Settings

Description

Set no packet Rx activity wait time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

wait-for-no-packet-rx 60

Syntax

diag advanced wireless

Mode

Config

Description

Configure advanced diag wireless settings.

Example

```
diag advanced wireless
```

Syntax

```
regulatory-domain
```

Mode

Diag Advanced Wireless Settings

Description

Enable wireless regulatory domain.

Example

```
regulatory-domain
```

Syntax

```
no regulatory-domain
```

Mode

Diag Advanced Wireless Settings

Description

Disbale wireless regulatory domain.

Example

```
no regulatory-domain
```

Syntax

```
sonicpoint support-type { all | sonicpoint-only | sonicpointn-only }
```

Mode

Diag Advanced Wireless Settings

Description

Set supported sonicPoint type.

Options

all	All types.
sonicpoint-only	Only support sonicpoint.
sonicpointn-only	Only support sonicpointn.

Example

```
sonicpoint support-type all
```

Syntax

```
sonicpoint self-maintenance { daily | weekly }
```

Mode

Diag Advanced Wireless Settings

Description

Set sonicpoint system self maintenance schedule.

Options

daily Maintenance 3:00AM every day.

weekly Maintenance 3:00AM every Sunday.

Example

```
sonicpoint self-maintenance daily
```

Syntax

```
no sonicpoint self-maintenance
```

Mode

Diag Advanced Wireless Settings

Description

Disbale sonicpoint system self maintenance.

Example

```
no sonicpoint self-maintenance
```

Syntax

```
vap-bssid-local-bit
```

Mode

Diag Advanced Wireless Settings

Description

Set local bit for virtual access point BSSID MAC address.

Example

```
vap-bssid-local-bit
```

Syntax

```
no vap-bssid-local-bit
```

Mode

Diag Advanced Wireless Settings

Description

Disable to set local bit for virtual access point BSSID MAC address.

Example

```
no vap-bssid-local-bit
```

Syntax

```
sonicpoint legacy-management
```

Mode

Diag Advanced Wireless Settings

Description

Enforce legacy SonicPoint-A/B/G and SonicPoint-G Only to be managed.

Example

```
sonicpoint legacy-management
```

Syntax

```
no sonicpoint legacy-management
```

Mode

Diag Advanced Wireless Settings

Description

Disable enforce legacy SonicPoint-A/B/G and SonicPoint-G Only to be managed.

Example

```
no sonicpoint legacy-management
```

Syntax

```
sonicpoint update-firmware
```

Mode

Diag Advanced Wireless Settings

Description

Update all sonicPoint firmware.

Example

```
sonicpoint update-firmware
```

Syntax

```
sonicpoint keepalive-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable sonicPoint keepalive enforcement.

Example

```
sonicpoint keepalive-enforcement
```

Syntax

```
no sonicpoint keepalive-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable sonicPoint keepalive enforcement.

Example

```
no sonicpoint keepalive-enforcement
```

Syntax

```
sonicpoint profile-tcp-window-size <UINT16>
```

Mode

Diag Advanced Wireless Settings

Description

Set sonicPoint provisioning profile TCP window size.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
sonicpoint profile-tcp-window-size 1400
```

Syntax

```
no sonicpoint profile-tcp-window-size
```

Mode

Diag Advanced Wireless Settings

Description

Clear sonicPoint provisioning profile TCP window size.

Example

```
sonicpoint profile-tcp-window-size 1400
```

Syntax

```
sonicpoint default-window-size
```

Mode

Diag Advanced Wireless Settings

Description

Use default TCP window size for sonicpointn provisioning protocol.

Example

```
sonicpoint default-window-size
```

Syntax

```
no sonicpoint default-window-size
```

Mode

Diag Advanced Wireless Settings

Description

Disable to use default TCP window size for sonicpointn provisioning protocol.

Example

```
no sonicpoint default-window-size
```

Syntax

```
sonicpointn ssh-management
```

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPointN SSH management.

Example

```
sonicpointn ssh-management
```

Syntax

```
no sonicpointn ssh-management
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPointN SSH management.

Example

```
no sonicpointn ssh-management
```

Syntax

```
sonicpointn logging
```

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPointN logging.

Example

```
sonicpointn logging
```

Syntax

```
no sonicpointn logging
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPointN logging.

Example

```
no sonicpointn logging
```

Syntax

```
sonicpoint erase-old-crash-log
```

Mode

Diag Advanced Wireless Settings

Description

Erase SonicPoint crash log generated by previous firmware image when SonicPoint image is updated.

Example

```
sonicpoint erase-old-crash-log
```

Syntax

```
no sonicpoint erase-old-crash-log
```

Mode

Diag Advanced Wireless Settings

Description

Disable to erase SonicPoint crash log generated by previous firmware image.

Example

```
no sonicpoint erase-old-crash-log
```

Syntax

```
sonicpointn noise-security-level { extremely-high | extremely-low | high | low | medium }
```

Mode

Diag Advanced Diagnostics Settings

Description

Set SonicPoint-Ni/Ne noise sensitivity level:
 (The higher noise sensitivity level should be selected when RF environment is getting noiser).

Options

extremely-high Extremely high.

extremely-low Extremely low.

high High.

low Low.

medium Medium.

Example

sonicpointn noise-security-level medium

Syntax

no sonicpointn noise-security-level

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPoint-Ni/Ne noise sensitivity.

Example

no sonicpointn noise-security-level

Syntax

sonicpointn noise-safemode-reboot

Mode

Diag Advanced Wireless Settings

Description

Reboot SonicPointN when noise safe mode detected.

Example

sonicpointn noise-safemode-reboot

Syntax

no sonicpointn noise-safemode-reboot

Mode

Diag Advanced Wireless Settings

Description

Disable to reboot SonicPointN when noise safe mode detected.

Example

no sonicpoint noise-safemode-reboot

Syntax

sonicpoint retain-ip

Mode

Diag Advanced Wireless Settings

Description

Enable SonicPoint(N) IP address retaining.

Example

sonicpoint retain-ip

Syntax

```
no sonicpoint retain-ip
```

Mode

Diag Advanced Wireless Settings

Description

Disable SonicPoint(N) IP address retaining.

Example

```
no sonicpoint retain-ip
```

Syntax

```
sonicpoint snap-header
```

Mode

Diag Advanced Wireless Settings

Description

Use SNAP packet between SonicPoint / SonicPointN and gateway.

Example

```
sonicpoint snap-header
```

Syntax

```
no sonicpoint snap-header
```

Mode

Diag Advanced Wireless Settings

Description

Disable to use SNAP packet between SonicPoint / SonicPointN and gateway.

Example

```
no sonicpoint snap-header
```

Syntax

```
sonicpoint fragment-icmp
```

Mode

Diag Advanced Wireless Settings

Description

Send need fragment ICMP packet to SonicPoint / SonicPointN client.

Example

```
sonicpoint fragment-icmp
```

Syntax

```
no sonicpoint fragment-icmp
```


Mode

Diag Advanced Wireless Settings

Description

Disable to send need fragment ICMP packet to SonicPoint / SonicPointN client.

Example

```
no sonicpoint fragment-icmp
```

Syntax

```
bonjour-intra-wlan
```

Mode

Diag Advanced Wireless Settings

Description

Enable intra-WLAN zone communication for bonjour packet.

Example

```
bonjour-intra-wlan
```

Syntax

```
no bonjour-intra-wlan
```

Mode

Diag Advanced Wireless Settings

Description

Disable intra-WLAN zone communication for bonjour packet.

Example

```
no bonjour-intra-wlan
```

Syntax

```
dhcp-arp-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

WLAN DHCP lease / ARP delivery success rate enhancement.

Example

```
dhcp-arp-enhancement
```

Syntax

```
no dhcp-arp-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

Disable WLAN DHCP lease / ARP delivery success rate enhancement.

Example

```
no dhcp-arp-enhancement
```

Syntax

```
guest-services-redirect-interval <UINT8>
```

Mode

Diag Advanced Wireless Settings

Description

Set wireless guest services redirect interval in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
guest-services-redirect-interval 15
```

Syntax

```
wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable legacy WiFiSec enforcement support.

Example

```
wifisec-enforcement
```

Syntax

```
no wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable legacy WiFiSec enforcement support.

Example

```
no wifisec-enforcement
```

Syntax

```
wlan reply-wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Enable applying WiFi security enforcement on reply traffic from WLAN to any other zone.

Example

```
wlan reply-wifisec-enforcement
```

Syntax

```
no wlan reply-wifisec-enforcement
```

Mode

Diag Advanced Wireless Settings

Description

Disable applying WiFi security enforcement on reply traffic from WLAN to any other zone.

Example

```
no wlan reply-wifisec-enforcement
```

Syntax

```
wlan dp-core-processing
```

Mode

Diag Advanced Wireless Settings

Description

Enable WLAN traffic DP core processing capability.

Example

```
wlan dp-core-processing
```

Syntax

```
no wlan dp-core-processing
```

Mode

Diag Advanced Wireless Settings

Description

Disable WLAN traffic DP core processing capability.

Example

```
no wlan dp-core-processing
```

Syntax

```
wlan broadcast-communication
```

Mode

Diag Advanced Wireless Settings

Description

Enable intra-WLAN zone communication for broadcast packet.

Example

```
wlan broadcast-communication
```

Syntax

```
no wlan broadcast-communication
```

Mode

Diag Advanced Wireless Settings

Description

Disable intra-WLAN Zone communication for broadcast packet.

Example

```
no wlan broadcast-communication
```

Syntax

```
wlan bypass-gateway-firewalling
```

Mode

Diag Advanced Wireless Settings

Description

Enable local wireless zone traffic to bypass gateway firewalling.

Example

```
wlan bypass-gateway-firewalling
```

Syntax

```
no wlan bypass-gateway-firewalling
```

Mode

Diag Advanced Wireless Settings

Description

Disable local wireless zone traffic to bypass gateway firewalling.

Example

```
no wlan bypass-gateway-firewalling
```

Syntax

```
wlan inter-client-communication
```

Mode

Diag Advanced Wireless Settings

Description

Enable easy inter-wireless client communications.

Example

wlan inter-client-communication

Syntax

no wlan inter-client-communication

Mode

Diag Advanced Wireless Settings

Description

Disable easy inter-wireless client communications.

Example

no wlan bypass-gateway-firewalling

Syntax

wlan ignore-check-ess

Mode

Diag Advanced Wireless Settings

Description

Ignore checking ESS capability flag for WLAN client.

Example

wlan ignore-check-ess

Syntax

no wlan ignore-check-ess

Mode

Diag Advanced Wireless Settings

Description

Disable ignore checking ESS capability flag for WLAN client.

Example

no wlan ignore-check-ess

Syntax

wlan legacy-intel-client

Mode

Diag Advanced Wireless Settings

Description

Enable legacy Intel wireless client connectivity support.

Example

wlan legacy-intel-client

Syntax

```
no wlan legacy-intel-client
```

Mode

Diag Advanced Wireless Settings

Description

Disable legacy Intel wireless client connectivity support.

Example

```
no wlan legacy-intel-client
```

Syntax

```
wlan nosiy-enviroment-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

Enable noisy environment wireless connectivity enhancement support.

Example

```
wlan nosiy-enviroment-enhancement
```

Syntax

```
no wlan nosiy-enviroment-enhancement
```

Mode

Diag Advanced Wireless Settings

Description

Disable noisy environment wireless connectivity enhancement support.

Example

```
no wlan nosiy-enviroment-enhancement
```

Syntax

```
wlan internal-dhcp
```

Mode

Diag Advanced Wireless Settings

Description

Enable creation of internal WLAN interface DHCP scope.

Example

```
wlan internal-dhcp
```

Syntax

```
no wlan internal-dhcp
```

Mode

Diag Advanced Wireless Settings

Description

Disable creation of internal WLAN interface DHCP scope.

Example

```
no wlan internal-dhcp
```

Syntax

```
diag advanced tooltip-no-description
```

Mode

Config

Description

Enable tooltip with no descriptions.

Example

```
diag advanced tooltip-no-description
```

Syntax

```
no diag advanced tooltip-no-description
```

Mode

Config

Description

Disable tooltip with no descriptions.

Example

```
no diag advanced tooltip-no-description
```

Syntax

```
diag advanced preference
```

Mode

Config

Description

Configure advanced diag preference conversion.

Example

```
diag advanced preference
```

Syntax

```
launching-conversion-control
```

Mode

Diag Advanced Preference Conversion

Description

Enable showing control for launching preference conversion window.

Example

```
launching-conversion-control
```

Syntax

```
no launching-conversion-control
```

Mode

Diag Advanced Preference Conversion

Description

Disable showing control for launching preference conversion window.

Example

```
no launching-conversion-control
```

Syntax

```
processor-server <HOSTNAME>
```

Mode

Diag Advanced Preference Conversion

Description

Set preference processor server.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
processor-server convert.global.sonicwall.com
```

Syntax

```
no processor-server
```

Mode

Diag Advanced Preference Conversion

Description

Clear preference processor server.

Example

```
no processor-server
```

Syntax

```
secure-http-to-processor
```

Mode

Diag Advanced Preference Conversion

Description

Enable using secure HTTP to connect to preference processor server.

Example

```
secure-http-to-processor
```

Syntax

```
no secure-http-to-processor
```

Mode

Diag Advanced Preference Conversion

Description

Disable using secure HTTP to connect to preference processor server.

Example

```
no secure-http-to-processor
```

Syntax

```
site-relative-directory <WORD>
```

Mode

Diag Advanced Preference Conversion

Description

Set site relative directory.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
site-relative-directory \"/popup\"
```

Syntax

```
no site-relative-directory
```

Mode

Diag Advanced Preference Conversion

Description

Clear site relative directory.

Example

```
no site-relative-directory
```

Syntax

```
check-when-importing
```

Mode

Diag Advanced Preference Conversion

Description

Enable checking when importing settings.

Example

```
check-when-importing
```

Syntax

```
no check-when-importing
```

Mode

Diag Advanced Preference Conversion

Description

Disable checking when importing settings.

Example

```
no check-when-importing
```

Syntax

```
diag advanced anti-spam
```

Mode

Config

Description

Configure advanced diag Anti-Spam.

Example

```
diag advanced anti-spam
```

Syntax

```
syn-flood-protection
```

Mode

Diag Advanced Anti-Spam

Description

Enable SYN flood protection for Anti-Spam-related connections.

Example

```
syn-flood-protection
```

Syntax

```
no syn-flood-protection
```

Mode

Diag Advanced Anti-Spam

Description

Disable SYN flood protection for Anti-Spam-related connections.

Example

```
no syn-flood-protection
```

Syntax

```
check-grid-ip-only
```

Mode

Diag Advanced Anti-Spam

Description

Use GRID IP reputation check only.

Example

```
check-grid-ip-only
```

Syntax

```
no check-grid-ip-only
```

Mode

Diag Advanced Anti-Spam

Description

Disable to use GRID IP reputation check only.

Example

```
no check-grid-ip-only
```

Syntax

```
outbound-smtp-grid-ip
```

Mode

Diag Advanced Anti-Spam

Description

Enable GRID IP reputation checking for outbound SMTP connections.

Example

```
outbound-smtp-grid-ip
```

Syntax

```
no outbound-smtp-grid-ip
```

Mode

Diag Advanced Anti-Spam

Description

Disable GRID IP reputation checking for outbound SMTP connections.

Example

```
no outbound-smtp-grid-ip
```

Syntax

```
disabling-custom-email
```

Mode

Diag Advanced Anti-Spam

Description

Enable disabling of custom user e-mail policies when Anti-spam is enabled.

Example

```
disabling-custom-email
```

Syntax

```
no disabling-custom-email
```

Mode

Diag Advanced Anti-Spam

Description

Disable disabling of custom user e-mail policies when Anti-Spam is enabled.

Example

```
no disabling-custom-email
```

Syntax

```
limited-admin-configuration
```

Mode

Diag Advanced Anti-Spam

Description

Enable allowing limited admin users to configure Anti-Spam service.

Example

```
limited-admin-configuration
```

Syntax

```
no limited-admin-configuration
```

Mode

Diag Advanced Anti-Spam

Description

Disable allowing limited admin users to configure Anti-Spam service.

Example

```
no limited-admin-configuration
```

Syntax

shlo-check

Mode

Diag Advanced Anti-Spam

Description

Enable SHLO check when Junk Store is unavailable (while E-mail Security is operational).

Example

shlo-check

Syntax

no shlo-check

Mode

Diag Advanced Anti-Spam

Description

Disable SHLO check when Junk Store is unavailable (while E-mail Security is operational).

Example

no shlo-check

Syntax

auto-generated-cass-acl

Mode

Diag Advanced Anti-Spam

Description

Enable editing of auto-generated CASS access rules.

Example

auto-generated-cass-acl

Syntax

no auto-generated-cass-acl

Mode

Diag Advanced Anti-Spam

Description

Disable editing of auto-generated CASS access rules.

Example

no auto-generated-cass-acl

Syntax

clear statistics

Mode

Diag Advanced Anti-Spam

Description

Clear statistics.

Example

clear statistics

Syntax

reset grid-name-cache

Mode

Diag Advanced Anti-Spam

Description

Reset GRID name cache.

Example

reset grid-name-cache

Syntax

no policies-and-objects

Mode

Diag Advanced Anti-Spam

Description

Deletes policies and objects.

Example

no policies-and-objects

Syntax

cass_cloud_service_addr { auto-resolve | static-ip <IPV4_HOST> }

Mode

Diag Advanced Anti-Spam

Description

Set CASS cloud service address.

Options

- auto-resolve** Resolve automatically.
- static-ip** Use this static IP address.
- <IPV4_HOST>** IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
cass_cloud_service_addr static-ip 204.212.170.13
```

Syntax

```
diag advanced hosted-email-security
```

Mode

Config

Description

Enable hosted e-mail security.

Example

```
diag advanced hosted-email-security
```

Syntax

```
no diag advanced hosted-email-security
```

Mode

Config

Description

Disable hosted e-mail security.

Example

```
no diag advanced hosted-email-security
```

Syntax

```
diag advanced email-detection
```

Mode

Config

Description

Enable e-mail system detection.

Example

```
diag advanced email-detection
```

Syntax

```
no diag advanced email-detection
```

Mode

Config

Description

Disable e-mail system detection.

Example

```
no diag advanced email-detection
```

Syntax

diag advanced remote-assistance

Mode

Config

Description

Enable remote assistance.

Example

diag advanced remote-assistance

Syntax

no diag advanced remote-assistance

Mode

Config

Description

Disable remote assistance.

Example

no diag advanced remote-assistance

Syntax

diag advanced sslvpn

Mode

Config

Description

Configure advanced diag SSL-VPN settings.

Example

diag advanced sslvpn

Syntax

netextender-version <WORD>

Mode

Diag Advanced SSL-VPN Settings

Description

Set NetExtender(for Windows) version.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

netextender-version TBD

Syntax

no netextender-version

Mode

Diag Advanced SSL-VPN Settings

Description

Clear NetExtender(for Windows) version.

Example

no netextender-version

Syntax

diag advanced backend-server

Mode

Config

Description

Configure advanced diag backend servers settings.

Example

diag advanced backend-server

Syntax

enable

Mode

Diag Advanced Backend Server Settings

Description

Enable communication with SonicWall backend servers.

Example

enable

Syntax

no enable

Mode

Diag Advanced Backend Server Settings

Description

Disable communication with SonicWall backend servers.

Example

no enable

Syntax

```
force-through { any | interface <ASSIGNED_INTERFACE> }
```

Mode

Diag Advanced Backend Server Settings

Description

Set interface to force communication with SonicWall backend servers going through.

Options

any	Any interface.
interface	Set interface.
<ASSIGNED_INTERFACE>	Interface name. Example: <i>X0</i>

Example

```
force-through interface X1
```

Syntax

```
diag advanced wan-acceleration
```

Mode

Config

Description

Configure advanced diag WAN acceleration.

Example

```
diag advanced wan-acceleration
```

Syntax

```
remote-checking
```

Mode

Diag Advanced Wan Acceleration

Description

Enable checking of connection responses by remote WAN acceleration device.

Example

```
remote-dev-connection-checking
```

Syntax

```
no remote-checking
```

Mode

Diag Advanced Wan Acceleration

Description

Disable checking of connection responses by remote WAN acceleration device.

Example

```
no remote-dev-connection-checking
```

Syntax

```
bypass-tcp-acceleration { failed-proxied-connection <UINT32> | short-lived-proxied-connection <UINT32> }
```

Mode

Diag Advanced Wan Acceleration

Description

Enable temporarily bypass TCP acceleration.

Options

<i>failed-proxied-connection</i> <i><UINT32></i>	Set temporarily bypass TCP acceleration for failed proxied connections (minutes). Integer in the form: D OR 0xHHHHHHHHH. Example: 123
<i>short-lived-proxied-connection</i> <i><UINT32></i>	Set temporarily bypass TCP acceleration for short-lived proxied connections (minutes). Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

```
bypass-tcp-acceleration failed-proxied-connection 15
```

Syntax

```
no bypass-tcp-acceleration { failed-proxied-connection | short-lived-proxied-connection }
```

Mode

Diag Advanced Wan Acceleration

Description

Disable temporarily bypass TCP acceleration.

Options

<i>failed-proxied-connection</i>	Set temporarily bypass TCP acceleration for failed proxied connections (minutes).
<i>short-lived-proxied-connection</i>	Set temporarily bypass TCP acceleration for short-lived proxied connections (minutes).

Example

```
no bypass-tcp-acceleration failed-proxied-connection
```

Syntax

```
skip-tcp-acceleration
```

Mode

Diag Advanced Wan Acceleration

Description

Skip TCP acceleration for stateful control channels (but accelerate data channels).

Example

skip-tcp-acceleration

Syntax

no skip-tcp-acceleration

Mode

Diag Advanced Wan Acceleration

Description

Disable skip TCP acceleration for stateful control channels (but accelerate data channels).

Example

no skip-tcp-acceleration

Syntax

clear debug-status

Mode

Diag Advanced Wan Acceleration

Description

Clear debug status.

Example

clear debug-status

Syntax

clear tcp-acceleration-database

Mode

Diag Advanced Wan Acceleration

Description

Clear TCP acceleration database.

Example

clear tcp-acceleration-database

Syntax

diag advanced geoip-location-service

Mode

Config

Description

Configure advanced diag GeoIP/Location service.

Example

diag advanced geoip-location-service

Syntax

```
remote-geoip-server { always | failed-resolution } [ default | ip <IPV4_HOST> ]
```

Mode

Diag Advanced GeoIP/Location Service

Description

Set location of remote GeoIP server address.

Options

<i>always</i>	Always use this IP for geoipdata.global.sonicwall.com.
<i>failed-resolution</i>	Use if geoipdata.global.sonicwall.com does not resolve.
<i>default</i>	Set the IP address to the default setting.
<i>ip</i> <IPV4_HOST>	Specify the IP address. IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
remote-geoip-server failed-resolution 204.212.170.189
```

Syntax

```
clear location-cache
```

Mode

Diag Advanced GeoIP/Location Service

Description

Clear location cache.

Example

```
clear location-cache
```

Syntax

```
use-control-plane
```

Mode

Diag Advanced GeoIP/Location Service

Description

Use control plane for GeoIP database lookups.

Example

```
use-control-plane
```

Syntax

```
no use-control-plane
```

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to use control plane for GeoIP database lookups.

Example

```
no use-control-plane
```

Syntax

```
bypass-geoip-blocking
```

Mode

Diag Advanced GeoIP/Location Service

Description

Bypass GeoIp blocking for stack initiated connections.

Example

```
bypass-geoip-blocking
```

Syntax

```
no bypass-geoip-blocking
```

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to bypass GeoIp blocking for stack initiated connections.

Example

```
no bypass-geoip-blocking
```

Syntax

```
bypass-botnet-blocking
```

Mode

Diag Advanced GeoIP/Location Service

Description

Bypass BOTNET blocking for stack initiated connections.

Example

```
bypass-botnet-blocking
```

Syntax

```
no bypass-botnet-blocking
```

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to bypass BOTNET blocking for stack initiated connections.

Example

```
no bypass-botnet-blocking
```

Syntax

```
geoip-botnet-map-file-upload
```

Mode

Diag Advanced GeoIP/Location Service

Description

Allow Geo-IP/Botnet filter map database file upload.

Example

```
geoip-botnet-map-file-upload
```

Syntax

```
no geoip-botnet-map-file-upload
```

Mode

Diag Advanced GeoIP/Location Service

Description

Disable to upload Geo-IP/Botnet filter map database file.

Example

```
no geoip-botnet-map-file-upload
```

Syntax

```
diag advanced flow-reporting
```

Mode

Config

Description

Configure advanced diag Flow Reporting.

Example

```
diag advanced flow-reporting
```

Syntax

```
clear location-map
```

Mode

Diag Advanced Flow Reporting

Description

Clear location map database.

Example

```
clear location-map
```

Syntax

export-raw-database

Mode

Diag Advanced Flow Reporting

Description

Enable export of raw flow-related database table entries.

Example

export-raw-database

Syntax

no export-raw-database

Mode

Diag Advanced Flow Reporting

Description

Disable export of raw flow-related database table entries.

Example

no export-raw-database

Syntax

sql-console

Mode

Diag Advanced Flow Reporting

Description

Enable SQL console in System > Diagnostics page.

Example

sql-console

Syntax

no sql-console

Mode

Diag Advanced Flow Reporting

Description

Disable SQL console in System > Diagnostics page.

Example

no sql-console

Syntax

```
appflow-monitor-browser-frame-launch
```

Mode

Diag Advanced Flow Reporting

Description

Enable launching of AppFlow monitor in a stand-alone browser frame.

Example

```
appflow-monitor-browser-frame-launch
```

Syntax

```
no appflow-monitor-browser-frame-launch
```

Mode

Diag Advanced Flow Reporting

Description

Disable launching of AppFlow monitor in a stand-alone browser frame.

Example

```
no appflow-monitor-browser-frame-launch
```

Syntax

```
non-admin-visualization
```

Mode

Diag Advanced Flow Reporting

Description

Enable visualization UI for Non-Admin/Config users.

Example

```
non-admin-visualization
```

Syntax

```
no non-admin-visualization
```

Mode

Diag Advanced Flow Reporting

Description

Disable visualization UI for Non-Admin/Config users.

Example

```
no non-admin-visualization
```

Syntax

```
database-busy-timeout <UINT32>
```

Mode

Diag Advanced Flow Reporting

Description

Set database busy timeout in msec.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

database-busy-timeout 3000

Syntax

no database-busy-timeout

Mode

Diag Advanced Flow Reporting

Description

Clear database busy timeout in msec.

Example

no database-busy-timeout

Syntax

hide-appflow-server

Mode

Diag Advanced Flow Reporting

Description

Hide AppFlow server feature.

Example

hide-appflow-server

Syntax

no hide-appflow-server

Mode

Diag Advanced Flow Reporting

Description

Disable to hide AppFlow server feature.

Example

no hide-appflow-server

Syntax

hide-gmsflow-server

Mode

Diag Advanced Flow Reporting

Description

Hide GmsFlow server feature.

Example

hide-gmsflow-server

Syntax

no hide-gmsflow-server

Mode

Diag Advanced Flow Reporting

Description

Disable to hide GmsFlow server feature.

Example

no hide-appflow-server

Syntax

report-server-address { ip <IPV4_HOST> | sonicwall }

Mode

Diag Advanced Flow Reporting

Description

Set appFlow reports server address.

Options

ip	Use this IP address for App reports upload.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

sonicwall	Connect to appreports.global.sonicwall.com.

Example

report-server-address ip 173.240.209.223

Syntax

https-upload

Mode

Diag Advanced Flow Reporting

Description

Use secure HTTP for AppFlow report upload.

Example

https-upload

Syntax

no https-upload

Mode

Diag Advanced Flow Reporting

Description

Disable to use secure HTTP for AppFlow report upload.

Example

no https-upload

Syntax

clear database-tables

Mode

Diag Advanced Flow Reporting

Description

Clear appflow database tables.

Example

clear database-tables

Syntax

diag advanced log-reschedule [interval <UINT16>]

Mode

Config

Description

Enable main log process reschedule and set interval.

Options

- interval*** Main log process reschedule interval.
- <UINT16>*** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

diag advanced log-reschedule-interval 100

Syntax

no diag advanced log-reschedule

Mode

Config

Description

Disable main log process reschedule.

Example

```
no diag advanced log-reschedule
```

Syntax

```
diag advanced ipv6 ready-enforce
```

Mode

Config

Description

Enable enforcement of IPv6 ready logo requirement.

Example

```
diag advanced ipv6 ready-enforce
```

Syntax

```
no diag advanced ipv6 ready-enforce
```

Mode

Config

Description

Disable enforcement of IPv6 ready logo requirement.

Example

```
no diag advanced ipv6 ready-enforce
```

Syntax

```
diag advanced ipv6 allow-ndp-packet-less-than-255
```

Mode

Config

Description

Allow NDP packet whose hop limit is less than 255.

Example

```
diag advanced ipv6 allow-ndp-packet-less-than-255
```

Syntax

```
no diag advanced ipv6 allow-ndp-packet-less-than-255
```

Mode

Config

Description

Do not allow NDP packet whose hop limit is less than 255.

Example

```
no diag advanced ipv6 allow-ndp-packet-less-than-255
```

Syntax

```
diag advanced ipv6 ndp-proxy-nat-ranges
```

Mode

Config

Description

Enable NDP proxy for NAT ranges.

Example

```
diag advanced ipv6 ndp-proxy-nat-ranges
```

Syntax

```
no diag advanced ipv6 ndp-proxy-nat-ranges
```

Mode

Config

Description

Disable NDP proxy for NAT ranges.

Example

```
no diag advanced ipv6 ndp-proxy-nat-ranges
```

Syntax

```
diag advanced icmp drop-unreachable-packet
```

Mode

Config

Description

Enable enforcement of dropping unreachable ICMP packet.

Example

```
diag advanced icmp drop-unreachable-packet
```

Syntax

```
no diag advanced icmp drop-unreachable-packet
```

Mode

Config

Description

Disable enforcement of dropping unreachable ICMP packet.

Example

```
no diag advanced icmp drop-unreachable-packet
```

Syntax

```
diag advanced icmp drop-exceeded-packet
```

Mode

Config

Description

Enable enforcement of dropping time exceed ICMP packet.

Example

```
diag advanced icmp drop-exceeded-packet
```

Syntax

```
no diag advanced icmp drop-exceeded-packet
```

Mode

Config

Description

Disable enforcement of dropping time exceed ICMP packet.

Example

```
no diag advanced icmp drop-exceeded-packet
```

Syntax

```
diag advanced debug suppress-task-lock
```

Mode

Config

Description

Suppress potential task lock warning message.

Example

```
diag advanced debug suppress-task-lock
```

Syntax

```
no diag advanced debug suppress-task-lock
```

Mode

Config

Description

Disable to suppress potential task lock message.

Example

```
no diag advanced debug suppress-task-lock
```

Syntax

```
diag advanced debug suppress-task-dead-warning
```

Mode

Config

Description

Suppress potential task dead loop warning message.

Example

```
diag advanced debug suppress-task-dead-warning
```

Syntax

```
no diag advanced debug suppress-task-dead-warning
```

Mode

Config

Description

Disable to suppress potential task dead loop warning message.

Example

```
no diag advanced debug suppress-task-dead-warning
```

Syntax

```
diag advanced debug suppress-performance-testing-warning
```

Mode

Config

Description

Suppress performance testing warning message.

Example

```
diag advanced debug suppress-performance-testing-warning
```

Syntax

```
no diag advanced debug suppress-performance-testing-warning
```

Mode

Config

Description

Disable to suppress performance testing warning message.

Example

```
no diag advanced debug suppress-performance-testing-warning
```

Syntax

```
diag advanced network-fo-1b
```

Mode

Config

Description

Configure advanced diag Network Failover and Load balancing.

Example

```
diag advanced network-fo-lb
```

Syntax

```
pers-idle-expire-time <UINT32>
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Set minutes to wait before removing idle entries from the Persistent LB Table.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
pers-idle-expire-time 15
```

Syntax

```
no pers-idle-expire-time
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

No wait idle entries from the Persistent LB Table.

Example

```
no pers-idle-expire-time
```

Syntax

```
pers-activity-interval <UINT32>
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Set seconds interval between inspections of the Persistent LB Table, for marking entries as idle.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
pers-activity-interval 15
```

Syntax

```
pers-reuse-max <UINT32>
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Set maximum reuse threshold for each entry in the Persistent LB Table, zero means unlimited.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
pers-reuse-max 15
```

Syntax

```
no pers-reuse-max
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

No maximum reuse threshold for each entry in the Persistent LB Table.

Example

```
no pers-reuse-max
```

Syntax

```
pers-src-ipaddr <IPV4_HOST>
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Set source IP Address to monitor (Source-Destination IP Binding to include in TSR).

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
pers-src-ipaddr 10.1.1.2
```

Syntax

```
no pers-src-ipaddr
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Clear source IP Address to monitor.

Example

```
no pers-src-ipaddr
```

Syntax

```
pers-dst-ipaddr <IPv4_HOST>
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Set destination IP Address to monitor (Source-Destination IP Binding to include in TSR).

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
pers-dst-ipaddr 10.1.1.2
```

Syntax

```
no pers-dst-ipaddr
```

Mode

Diag Advanced Network Failover and Load Balance Settings

Description

Clear destination IP Address to monitor.

Example

```
no pers-dst-ipaddr
```

Syntax

```
diag advanced trace-log
```

Mode

Config

Description

Configure advanced diag trace log.

Example

```
diag advanced trace-log
```

Syntax

```
cpu-util-check
```

Mode

Diag Advanced trace log Configuration

Description

Enable CPU utilization check.

Example

```
cpu-util-check
```

Syntax

```
no cpu-util-check
```

Mode

Diag Advanced trace log Configuration

Description

Disable CPU utilization check.

Example

```
no cpu-util-check
```

Syntax

```
cpu-util-threshold <UINT16>
```

Mode

Diag Advanced trace log Configuration

Description

Set CPU utilization expectation threshold.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
cpu-util-threshold 10
```

Syntax

```
no cpu-util-threshold
```

Mode

Diag Advanced trace log Configuration

Description

set CPU utilization expectation threshold value to 0.

Example

```
no cpu-util-threshold
```

Syntax

```
clear trace-log { all | all-current | current | last }
```

Mode

Diag Advanced trace log Configuration

Description

Clear trace log.

Options

<i>all</i>	Clear all trace log information.
<i>all-current</i>	Clear all-current trace log information.
<i>current</i>	Clear current trace log information.
<i>last</i>	Clear last trace log information.

Example

```
clear trace-log current
clear trace-log all
clear trace-log last
clear trace-log all-current
```

Syntax

```
diag advanced fqdn-dyn-addr-obj
```

Mode

Config

Description

Configure advanced diag FQDN dynamic address object.

Example

```
diag advanced fqdn-dyn-addr-obj
```

Syntax

```
cache-dns-reply
```

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable FQDN object only cache DNS reply from sanctioned server.

Example

```
cache-dns-reply
```

Syntax

```
no cache-dns-reply
```

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable FQDN object only cache DNS reply from sanctioned server.

Example

```
no cache-dns-reply
```

Syntax

offset-for-fqdn-objects <UINT16>

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Offset for FQDN objects(seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

offset-for-fqdn-objects 10

Syntax

no offset-for-fqdn-objects

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Set offset for FQDN objects(seconds) value to 0.

Example

no offset-for-fqdn-objects

Syntax

refresh-sub-domains

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable refresh sub domains of wildcard FQDN dynamic address objects.

Example

refresh-sub-domains

Syntax

no refresh-sub-domains

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable refresh sub domains of wildcard FQDN dynamic address objects.

Example

no refresh-sub-domains

Syntax

donot-delete-expired-hosts

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable donot delete expired hosts of an FQDN network object with active connections.

Example

donot-delete-expired-hosts

Syntax

no donot-delete-expired-hosts

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable donot delete expired hosts of an FQDN network object with active connections.

Example

no donot-delete-expired-hosts

Syntax

retain-expired-fqdn-hosts

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable retain expired FQDN hosts until a successfull DNS resolutions occurs.

Example

retain-expired-fqdn-hosts

Syntax

no retain-expired-fqdn-hosts

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable retain expired FQDN hosts until a successfull DNS resolutions occurs.

Example

no retain-expired-fqdn-hosts

Syntax

unlimited-queries

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable unlimited queries to resolve custom FQDN objects.

Example

unlimited-queries

Syntax

no unlimited-queries

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable unlimited queries to resolve custom FQDN objects.

Example

no unlimited-queries

Syntax

stop-dns-queries

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Enable stop dns queries for default FQDN objects after maximumthreshold.

Example

stop-dns-queries

Syntax

no stop-dns-queries

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Disable stop dns queries for default FQDN objects after maximumthreshold.

Example

no stop-dns-queries

Syntax

max-retry-threshold <UINT16>

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

FQDN maximum retry threshold before stopping query.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-retry-threshold 10
```

Syntax

```
min-allowed-ttl <UINT16>
```

Mode

Diag Advanced FQDN dynamic address object Configuration

Description

Minimum allowed ttl for FQDN objects.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
min-allowed-ttl 10
```

Syntax

```
diag advanced cta-report
```

Mode

Config

Description

Configure advanced diag capture threat assessment report.

Example

```
diag advanced cta-report
```

Syntax

```
use-secure-http
```

Mode

Diag Advanced capture threat assessment report

Description

Enable use secure http to communicate to the service.

Example

```
use-secure-http
```

Syntax

```
no use-secure-http
```

Mode

Diag Advanced capture threat assessment report

Description

Disable use secure http to communicate to the service.

Example

```
no use-secure-http
```

Syntax

```
service-address type { resolve-automatically | static-ip }
```

Mode

Diag Advanced capture threat assessment report

Description

select the service address type.

Options

resolve-automatically Service address type as resolve-automatically.

static-ip Service address type as atatic IP.

Example

```
service-address type resolve-automatically
```

Syntax

```
service-address ip <IPV4_HOST>
```

Mode

Diag Advanced capture threat assessment report

Description

set the service address ip.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
service-address ip 2.3.4.5
```

Syntax

```
no service-address ip
```

Mode

Diag Advanced capture threat assessment report

Description

set the service address ip to 0.0.0.0.

Example

```
no service-address ip
```

Syntax

```
service-http-port <UINT32>
```

Mode

Diag Advanced capture threat assessment report

Description

Set the service HTTP port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
service-http-port 3443
```

Syntax

```
no service-http-port
```

Mode

Diag Advanced capture threat assessment report

Description

Set the service HTTP port to 0.

Example

```
no service-http-port
```

Syntax

```
service-https-port <UINT32>
```

Mode

Diag Advanced capture threat assessment report

Description

Set the service HTTPS port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
service-https-port 3443
```

Syntax

```
no service-https-port
```

Mode

Diag Advanced capture threat assessment report

Description

Set the service HTTPS port to 0.

Example

```
no service-https-port
```

Syntax

```
upload-to-cloud-service
```

Mode

Diag Advanced capture threat assessment report

Description

Enable upload to cloud service.

Example

```
upload-to-cloud-service
```

Syntax

```
no upload-to-cloud-service
```

Mode

Diag Advanced capture threat assessment report

Description

Disable upload to cloud service.

Example

```
no upload-to-cloud-service
```

Syntax

```
upload-to-yaml-format
```

Mode

Diag Advanced capture threat assessment report

Description

Enable upload to YAML format.

Example

```
upload-to-yaml-format
```

Syntax

```
no upload-to-yaml-format
```

Mode

Diag Advanced capture threat assessment report

Description

Disable upload to YAML format.

Example

no upload-to-yaml-format

Syntax

support-for-ctav1-only

Mode

Diag Advanced capture threat assessment report

Description

Enable support for CTAV1 only.

Example

support-for-ctav1-only

Syntax

no support-for-ctav1-only

Mode

Diag Advanced capture threat assessment report

Description

Disable support for CTAV1 only.

Example

no support-for-ctav1-only

Syntax

csc-reporting-cloud-fqdn <WORD>

Mode

Diag Advanced capture threat assessment report

Description

Set csc reporting cloud fqdn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

csc-reporting-cloud-fqdn

Syntax

```
no csc-reporting-cloud-fqdn
```

Mode

Diag Advanced capture threat assessment report

Description

Clear csc reporting cloud fqdn.

Example

```
no csc-reporting-cloud-fqdn
```

Syntax

```
diag advanced zero-touch
```

Mode

Config

Description

Configure advanced diag Zero Touch settings.

Example

```
diag advanced zero-touch
```

Syntax

```
restart
```

Mode

Diag Advanced Zero Touch Settings

Description

Restart Zero Touch.

Example

```
restart
```

Syntax

```
enable
```

Mode

Diag Advanced Zero Touch Settings

Description

Enable Zero Touch.

Example

```
enable
```

Syntax

```
disable
```

Mode

Diag Advanced Zero Touch Settings

Description

Disable Zero Touch.

Example

```
disable
```

Syntax

```
fqdn-server <WORD>
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the Server FQDN.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
fqdn-server cloudtt.global.sonicwall.com
```

Syntax

```
server-ip-use-mode { always-use | use-when-unresolved }
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the Server IP Use Mode.

Options

always-use Configure the Server IP Use Mode.

use-when-unresolved Configure the Server IP Use Mode.

Example

```
server-ip-use-mode use-when-unresolved
```

Syntax

```
server-ip <IPV4_HOST>
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the Server IP.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.

Example: 192.168.168.168

Example

```
server-ip 0.0.0.0
```

Syntax

```
no server-ip
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the Server IP.

Example

```
no server-ip
```

Syntax

```
reconnecting-delay <UINT32>
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the reconnecting delay in Seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
reconnecting-delay 10
```

Syntax

```
no reconnecting-delay
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the reconnecting delay in Seconds.

Example

```
no reconnecting-delay
```

Syntax

```
reconnecting-attempt <UINT32>
```

Mode

Diag Advanced Zero Touch Settings

Description

Configure the reconnecting attempt.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

reconnecting-attempt 10

Syntax

no reconnecting-attempt

Mode

Diag Advanced Zero Touch Settings

Description

Configure the reconnecting attempt.

Example

no reconnecting-attempt

Syntax

skip-certificate

Mode

Diag Advanced Zero Touch Settings

Description

Enable Skip checking server certificate.

Example

skip-certificate

Syntax

no skip-certificate

Mode

Diag Advanced Zero Touch Settings

Description

Disable Skip checking server certificate.

Example

no skip-certificate

Syntax

show-diagnostic-page

Mode

Description

Enable the show diagnostic page.

Example

show-diagnostic-page

Syntax

no show-diagnostic-page

Mode

Diag Advanced Zero Touch Settings

Description

Disable the show diagnostic page.

Example

no show-diagnostic-page

Syntax

debug-level <UINT32>

Mode

Diag Advanced Zero Touch Settings

Description

Configure the debug level.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

debug-level 1

Syntax

no debug-level

Mode

Diag Advanced Zero Touch Settings

Description

Configure the debug level.

Example

no debug-level

Syntax

memory-free-call-tracking [hash-size-exponent <UINT32>] [record-up-to <UINT32>]

Mode

Diag Advanced Diagnostics Settings

Description

Enable tracking of memory free calls for double-free detection.

Options

- hash-size-exponent***
<UINT32>

Set the exponent value controlling the size of the tracking table.
Integer in the form: D OR 0xHHHHHHHH.
Example: 123
- record-up-to***
<UINT32>

Set the number of previous free calls to record for each memory address.
Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

memory-free-call-tracking

Syntax

no memory-free-call-tracking

Mode

Diag Advanced Diagnostics Settings

Description

Disable tracking of memory free calls for double-free detection.

Example

no memory-free-call-tracking

Syntax

packet-monitor

Mode

Config

Description

Configure packet monitor settings.

Example

packet-monitor

Syntax

start capture

Mode

Packet Monitor
Top Level
Config

Description

Start packet capture.

Example

start capture

Syntax

stop capture

Mode

Packet Monitor
Top Level
Config

Description

Stop packet capture.

Example

stop capture

Syntax

start mirror

Mode

Packet Monitor
Top Level
Config

Description

Start mirror.

Example

start mirror

Syntax

stop mirror

Mode

Packet Monitor
Top Level
Config

Description

Stop mirror.

Example

stop mirror

Syntax

log-to-ftp

Mode

Packet Monitor
Top Level
Config

Description

Packet monitor log to FTP server.

Example

```
log-to-ftp
```

Syntax

```
export capture { app-data | html | libpcap | pcapng | text } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Packet Monitor

Description

Export capture from the device using ftp.

Options

app-data	App data.
html	HTML.
libpcap	LibPcap.
pcapng	PcapNG.
text	Text.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export capture libpcap ftp ftp://user:password@ftp.myserver.local/capture.cap
export capture libpcap scp user@server:/home/user/capture.cap
export capture libpcap scp user@server:/home/user
```

Syntax

```
monitor all
```

Mode

Top Level
Config
Packet Monitor

Description

Monitor all packets.

Example

```
monitor all
```

Syntax

monitor default

Mode

Packet Monitor
Top Level
Config

Description

Set packet monitor settings to default.

Example

monitor default

Syntax

clear capture

Mode

Packet Monitor
Top Level
Config

Description

Clear the packet capture buffer.

Example

clear capture

Syntax

bytes-to-capture <UINT16>

Mode

Packet Monitor

Description

Specify number of bytes to capture (per packet).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

bytes-to-capture 1520

Syntax

wrap-buffer

Mode

Packet Monitor

Description

Enable wrapping of capture buffer once full.

Example

wrap-buffer

Syntax

no wrap-buffer

Mode

Packet Monitor

Description

Disable wrapping of capture buffer once full.

Example

no wrap-buffer

Syntax

exclude encrypted-gms

Mode

Packet Monitor

Description

Enable exclusion of encrypted GMS traffic.

Example

exclude encrypted-gms

Syntax

no exclude encrypted-gms

Mode

Packet Monitor

Description

Disable exclusion of encrypted GMS traffic.

Example

no exclude encrypted-gms

Syntax

exclude management { http | snmp | ssh }

Mode

Packet Monitor

Description

Enable exclusion of specified management.

Options

http HTTP/HTTPS.

snmp SNMP.

ssh SSH.

Example

```
exclude management http ssh
```

Syntax

```
no exclude management { http | snmp | ssh }
```

Mode

Packet Monitor

Description

Disable exclusion of specified management.

Options

http HTTP/HTTPS.

snmp SNMP.

ssh SSH.

Example

```
no exclude management http ssh
```

Syntax

```
exclude syslog { gms-server | syslog-servers }
```

Mode

Packet Monitor

Description

Enable exclusion of syslog traffic to specified server(s).

Options

gms-server GMS server.

syslog-servers Sylog servers.

Example

```
exclude syslog syslog-servers
```

Syntax

```
no exclude syslog { gms-server | syslog-servers }
```

Mode

Packet Monitor

Description

Disable exclusion of syslog traffic to specified server(s).

Options

gms-server GMS server.

syslog-servers Sylog servers.

Example

```
no exclude syslog syslog-servers
```

Syntax

```
exclude internal-traffic { ha | sonicpoint }
```

Mode

Packet Monitor

Description

Enable exclusion of internal traffic.

Options

ha High availability.

sonicpoint SonicPoint.

Example

```
exclude internal-traffic ha
```

Syntax

```
no exclude internal-traffic { ha | sonicpoint }
```

Mode

Packet Monitor

Description

Disable exclusion of internal traffic.

Options

ha High availability.

sonicpoint SonicPoint.

Example

```
no exclude internal-traffic internal-servers
```

Syntax

```
monitor-filter based-on-firewall-rule
```

Mode

Packet Monitor

Description

Enable packet monitor filter based on the firewall access/app rules.

Example

```
monitor-filter based-on-firewall-rule
```

Syntax

```
no monitor-filter based-on-firewall-rule
```

Mode

Packet Monitor

Description

Disable packet monitor filter based on the firewall access/app rules.

Example

```
no monitor-filter based-on-firewall-rule
```

Syntax

```
monitor-filter interfaces <WORD>
```

Mode

Packet Monitor

Description

Specify name of interface(s) on which packet capture needs to be performed (maximum 10).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter interfaces "X0,X1,X2:V100"  
monitor-filter interfaces "!X0,!X1"
```

Syntax

```
no monitor-filter interfaces
```

Mode

Packet Monitor

Description

Clear name of interface(s) on which packet capture needs to be performed.

Example

```
no monitor-filter interfaces
```

Syntax

```
monitor-filter ether-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ether type(s) on which packet capture needs to be performed. Currently ARP(arp), IP(ip), PPPoE-SES, PPPoE-DIS or you can specify the value directly in hex format like 0x800.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter ether-types "ARP,ip,0x800"  
monitor-filter ether-types "!ARP,!0x800"
```

Syntax

```
no monitor-filter ether-types
```

Mode

Packet Monitor

Description

Clear name of ether type(s) on which packet capture needs to be performed.

Example

```
no monitor-filter ether-types
```

Syntax

```
monitor-filter ip-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ip type(s) on which packet capture needs to be performed. Currently TCP, UDP, ICMP, GRE, IGMP, AH, ESP or you can specify the value directly in hex format like 0x6.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter ip-types "TCP,UDP,0x6"  
monitor-filter ip-types "!TCP,!0x6"
```

Syntax

```
no monitor-filter ip-types
```

Mode

Packet Monitor

Description

Clear name of ip type(s) on which packet capture needs to be performed.

Example

```
no monitor-filter ip-types
```

Syntax

```
monitor-filter source-ips <WORD>
```

Mode

Packet Monitor

Description

Specify source IP addresses on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter source-ips "10.10.10.1,10.10.10.3,10.10.10.7"  
monitor-filter source-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no monitor-filter source-ips
```

Mode

Packet Monitor

Description

Clear source IP addresses on which packet capture needs to be performed.

Example

```
no monitor-filter source-ips
```

Syntax

```
monitor-filter source-ports <WORD>
```

Mode

Packet Monitor

Description

Specify source TCP/UDP ports on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter source-ports "20,75,80"
```

Syntax

```
no monitor-filter source-ports
```

Mode

Packet Monitor

Description

Clear source TCP/UDP ports on which packet capture needs to be performed.

Example

```
no monitor-filter source-ports
```

Syntax

```
monitor-filter destination-ips <WORD>
```

Mode

Packet Monitor

Description

Specify destination IP addresses on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter destination-ips "10.10.10.1,10.10.10.7"  
monitor-filter destination-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no monitor-filter destination-ips
```

Mode

Packet Monitor

Description

Clear destination IP addresses on which packet capture needs to be performed.

Example

```
no monitor-filter destination-ips
```

Syntax

```
monitor-filter destination-ports <WORD>
```

Mode

Packet Monitor

Description

Specify destination TCP/UDP ports on which packet capture needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
monitor-filter destination-ports "20,75,80"  
monitor-filter destination-ports "!20,!80"
```

Syntax

```
no monitor-filter destination-ports
```

Mode

Packet Monitor

Description

Clear destination TCP/UDP ports on which packet capture needs to be performed.

Example

```
no monitor-filter destination-ports
```

Syntax

```
monitor-filter bidirectional
```

Mode

Packet Monitor

Description

Enable bidirectional address and port matching.

Example

```
monitor-filter bidirectional
```

Syntax

```
no monitor-filter bidirectional
```

Mode

Packet Monitor

Description

Disable bidirectional address and port matching.

Example

```
no monitor-filter bidirectional
```

Syntax

```
monitor-filter status { consumed | dropped | forwarded }
```

Mode

Packet Monitor

Description

Enable monitor filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

Example

monitor-filter status forwarded

Syntax

no monitor-filter status { consumed | dropped | forwarded }

Mode

Packet Monitor

Description

Disable monitor filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

Example

no monitor-filter status forwarded

Syntax

display-filter interfaces <WORD>

Mode

Packet Monitor

Description

Specify name of interface(s) on which packet filter needs to be performed (maximum 10).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

display-filter interfaces "X0,X1,X2:V100"
display-filter interfaces "!X0,!X1"

Syntax

no display-filter interfaces

Mode

Packet Monitor

Description

Clear name of interface(s) on which packet filter needs to be performed.

Example

no display-filter interfaces

Syntax

```
display-filter ether-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ether type(s) on which packet filter needs to be performed. Currently ARP(arp), IP(ip), PPPoE-SES, PPPoE-DIS or you can specify the value directly in hex format like 0x800.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter ether-types "ARP,ip,0x800"  
display-filter ether-types "!ARP,!0x800"
```

Syntax

```
no display-filter ether-types
```

Mode

Packet Monitor

Description

Clear name of ether type(s) on which packet filter needs to be performed.

Example

```
no display-filter ether-types
```

Syntax

```
display-filter ip-types <WORD>
```

Mode

Packet Monitor

Description

Specify name of ip type(s) on which packet filter needs to be performed. Currently TCP, UDP, ICMP, GRE, IGMP, AH, ESP or you can specify the value directly in hex format like 0x6.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter ip-types "TCP,UDP,0x6"  
display-filter ip-types "!TCP,!0x6"
```

Syntax

```
no display-filter ip-types
```

Mode

Packet Monitor

Description

Clear name of ip type(s) on which packet filter needs to be performed.

Example

```
no display-filter ip-types
```

Syntax

```
display-filter source-ips <WORD>
```

Mode

Packet Monitor

Description

Specify source IP addresses on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter source-ips "10.10.10.1,10.10.10.7"  
display-filter source-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no display-filter source-ips
```

Mode

Packet Monitor

Description

Clear source IP addresses on which packet filter needs to be performed.

Example

```
no display-filter source-ips
```

Syntax

```
display-filter source-ports <WORD>
```

Mode

Packet Monitor

Description

Specify source TCP/UDP ports on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter source-ports "20,75,80"  
display-filter source-ports "!20,!80"
```

Syntax

```
no display-filter source-ports
```

Mode

Packet Monitor

Description

Clear source TCP/UDP ports on which packet filter needs to be performed.

Example

```
no display-filter source-ports
```

Syntax

```
display-filter destination-ips <WORD>
```

Mode

Packet Monitor

Description

Specify destination IP addresses on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter destination-ips "10.10.10.1,10.10.10.7"  
display-filter destination-ips "!10.10.10.1,!10.10.10.3"
```

Syntax

```
no display-filter destination-ips
```

Mode

Packet Monitor

Description

Clear destination IP addresses on which packet filter needs to be performed.

Example

```
no display-filter destination-ips
```

Syntax

```
display-filter destination-ports <WORD>
```

Mode

Packet Monitor

Description

Specify destination TCP/UDP ports on which packet filter needs to be performed.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
display-filter destination-ports "20,75,80"  
display-filter destination-ports "!20,!80"
```

Syntax

```
no display-filter destination-ports
```

Mode

Packet Monitor

Description

Clear destination TCP/UDP ports on which packet filter needs to be performed.

Example

```
no display-filter destination-ports
```

Syntax

```
display-filter bidirectional
```

Mode

Packet Monitor

Description

Enable bidirectional address and port matching.

Example

```
display-filter bidirectional
```

Syntax

```
no display-filter bidirectional
```

Mode

Packet Monitor

Description

Disable bidirectional address and port matching.

Example

```
no display-filter bidirectional
```

Syntax

```
display-filter status { consumed | dropped | forwarded | generated }
```

Mode

Packet Monitor

Description

Enable display filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

generated Generated.

Example

```
display-filter status forwarded generated
```

Syntax

```
no display-filter status { consumed | dropped | forwarded | generated }
```

Mode

Packet Monitor

Description

Disable display filtering for the specified status.

Options

consumed Consumed.

dropped Dropped.

forwarded Forwarded.

generated Generated.

Example

```
no display-filter status forwarded generated
```

Syntax

```
ftp server <IPV4_HOST>
```

Mode

Packet Monitor

Description

Specify the FTP server's IP address to send the packet capture to.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ftp server 192.168.168.75
```

Syntax

```
no ftp server
```

Mode

Packet Monitor

Description

Clear the FTP server's IP address.

Example

```
no ftp server
```

Syntax

```
ftp login <WORD>
```

Mode

Packet Monitor

Description

Specify the FTP server's login name to send the packet capture.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp login admin@testing.local
```

Syntax

```
no ftp login
```

Mode

Packet Monitor

Description

Clear the FTP server's login name.

Example

```
no ftp login
```

Syntax

```
ftp password <ENC_PASSWORD>
```

Mode

Packet Monitor

Description

Specify the FTP server's login password to send the packet capture.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
ftp password myftppassword
```

Syntax

```
no ftp password
```

Mode

Packet Monitor

Description

Clear the FTP server's login password.

Example

```
no ftp password
```

Syntax

```
ftp directory <WORD>
```

Mode

Packet Monitor

Description

Specify the FTP server's directory to place the packet capture in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp directory captures/firewall/
```

Syntax

```
no ftp directory
```

Mode

Packet Monitor

Description

Clear the FTP server's directory.

Example

```
no ftp directory
```

Syntax

```
ftp automatic
```

Mode

Packet Monitor

Description

Enable automatically log captures to the FTP server.

Example

```
ftp automatic
```

Syntax

```
no ftp automatic
```

Mode

Packet Monitor

Description

Disable automatically log captures to the FTP server.

Example

```
no ftp automatic
```

Syntax

```
ftp pcapng
```

Mode

Packet Monitor

Description

Enable logging of PCAPNG file.

Example

```
ftp pcapng
```

Syntax

```
no ftp pcapng
```

Mode

Packet Monitor

Description

Disable logging of PCAPNG file.

Example

```
no ftp pcapng
```

Syntax

```
ftp html
```

Mode

Packet Monitor

Description

Enable logging of HTML file along with .cap file.

Example

```
ftp html
```

Syntax

```
no ftp html
```

Mode

Packet Monitor

Description

Disable logging of HTML file along with .cap file.

Example

```
no ftp html
```

Syntax

```
monitor-filter firewall-generated
```

Mode

Packet Monitor

Description

Enable monitoring of firewall generated packets. (This will bypass interface filter).

Example

```
monitor-filter firewall-generated
```

Syntax

```
no monitor-filter firewall-generated
```

Mode

Packet Monitor

Description

Disable monitoring of firewall generated packets. (This will bypass interface filter).

Example

```
no monitor-filter firewall-generated
```

Syntax

```
monitor-filter intermediate [ fragmented | intermediate-packets | iphelper | ipsec | ldap-over-tls | multicast | reassembled | remote-mirrored | restore-ports-ssl | ssl | sso-agent ]
```

Mode

Packet Monitor

Description

Enable monitoring of intermediate packet.

Options

<i>fragmented</i>	Enable monitoring of intermediate fragmented traffic.
<i>intermediate-packets</i>	Enable monitoring intermediate packets.
<i>iphelper</i>	Enable monitoring of intermediate IP helper traffic.
<i>ipsec</i>	Enable monitoring of intermediate IPSEC traffic.

<i>ldap-over-tls</i>	Enable monitoring of intermediate decrypted LDAP over TLS traffic.
<i>multicast</i>	Enable monitoring of intermediate multicast traffic.
<i>reassembled</i>	Enable monitoring of intermediate reassembled traffic.
<i>remote-mirrored</i>	Enable monitoring of intermediate remote mirrored traffic.
<i>restore-ports-ssl</i>	Enable restore original ports on SSL decrypted traffic.
<i>ssl</i>	Enable monitoring of intermediate SSL decrypted traffic.
<i>sso-agent</i>	Enable monitoring of intermediate decrypted Single Sign On agent messages.

Example

```
monitor-filter intermediate ipsec
```

Syntax

```
no monitor-filter intermediate [ fragmented | intermediate-packets | iphelper | ipsec | ldap-over-tls | multicast | reassembled | remote-mirrored | restore-ports-ssl | ssl | sso-agent ]
```

Mode

Packet Monitor

Description

Disable monitoring of intermediate packet.

Options

<i>fragmented</i>	Disable monitoring of intermediate fragmented traffic.
<i>intermediate-packets</i>	Disable monitoring intermediate packets.
<i>iphelper</i>	Disable monitoring of intermediate IP helper traffic.
<i>ipsec</i>	Disable monitoring of intermediate IPSEC traffic.
<i>ldap-over-tls</i>	Disable monitoring of intermediate decrypted LDAP over TLS traffic.
<i>multicast</i>	Disable monitoring of intermediate multicast traffic.
<i>reassembled</i>	Disable monitoring of intermediate reassembled traffic.
<i>remote-mirrored</i>	Disable monitoring of intermediate remote mirrored traffic.
<i>restore-ports-ssl</i>	Disable restore original ports on SSL decrypted traffic.
<i>ssl</i>	Disable monitoring of intermediate SSL decrypted traffic.
<i>sso-agent</i>	Disable monitoring of intermediate decrypted Single Sign On agent messages.

Example

```
no monitor-filter intermediate ipsec
```

Syntax

```
mirror max-rate <UINT32>
```

Mode

Packet Monitor

Description

Set maximum mirror rate (in kilobits per second).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
mirror max-rate 100
```

Syntax

```
mirror only-ip-packets
```

Mode

Packet Monitor

Description

Enable mirror only IP packets.

Example

```
mirror only-ip-packets
```

Syntax

```
no mirror only-ip-packets
```

Mode

Packet Monitor

Description

Disable mirror only IP packets.

Example

```
no mirror only-ip-packets
```

Syntax

```
mirror interface <PACKET_MONITOR_MIRROR_INTERFACE>
```

Mode

Packet Monitor

Description

Mirror filtered packets to interface.

Options

<PACKET_MONITOR_MIRROR_INTERFACE> Interface name.
Example: X0

Example

```
mirror interface X3
```

Syntax

```
no mirror interface
```

Mode

Packet Monitor

Description

Disable mirror filtered packets to interface (NSA platforms only).

Example

```
no mirror interface
```

Syntax

```
mirror ip <IPV4_HOST>
```

Mode

Packet Monitor

Description

Mirror filtered packets to remote SonicWall firewall (IP address).

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
mirror ip 10.11.10.10
```

Syntax

```
no mirror ip
```

Mode

Packet Monitor

Description

Disable mirror filtered packets to remote SonicWall firewall (IP address).

Example

```
no mirror ip
```

Syntax

```
mirror receive-from-ip <IPV4_HOST>
```

Mode

Packet Monitor

Description

Receive mirrored packets from remote SonicWall firewall (IP address).

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
mirror receive-from-ip 10.11.10.10
```

Syntax

```
no mirror receive-from-ip
```

Mode

Packet Monitor

Description

Disable receive mirrored packets from remote SonicWall firewall (IP address).

Example

```
no mirror receive-from-ip
```

Syntax

```
mirror forward-interface <PACKET_MONITOR_MIRROR_INTERFACE>
```

Mode

Packet Monitor

Description

Send received remote mirrored packets to interface.

Options

<PACKET_MONITOR_MIRROR_INTERFACE> Interface name.
Example: X0

Example

```
mirror forward-interface X2
```

Syntax

```
no mirror forward-interface
```

Mode

Packet Monitor

Description

Mirror filtered packets to interface.

Example

```
no mirror forward-interface
```

Syntax

```
mirror to-capture-buffer
```

Mode

Packet Monitor

Description

Enable sending received remote mirrored packets to capture buffer.

Example

```
mirror to-capture-buffer
```

Syntax

```
no mirror to-capture-buffer
```

Mode

Packet Monitor

Description

Disable sending received remote mirrored packets to capture buffer.

Example

```
no mirror to-capture-buffer
```

Syntax

```
mirror encrypt-key <WORD>
```

Mode

Packet Monitor

Description

Encrypt remote mirrored packets via IPSec (preshared key-IKE).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mirror encrypt-key
```

Syntax

```
mirror decrypt-key <WORD>
```

Mode

Packet Monitor

Description

Decrypt remote mirrored packets via IPSec (preshared key-IKE).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
mirror encrypt-key
```

Syntax

send tech-support-report

Mode

Config
Top Level

Description

Send tech support report to MySonicwall.

Example

send tech-support-report

Syntax

tech-support-report options

Mode

Config

Description

Configure tech support report options.

Example

tech-support-report options

Syntax

sensitive-keys

Mode

TSR options

Description

Enable display of sensitive keys in tech support report.

Example

sensitive-keys

Syntax

no sensitive-keys

Mode

TSR options

Description

Disable display of sensitive keys in tech support report.

Example

no sensitive-keys

Syntax

arp-cache

Mode

TSR options

Description

Enable display of ARP cache in tech support report.

Example

arp-cache

Syntax

no arp-cache

Mode

TSR options

Description

Disable display of ARP cache in tech support report.

Example

no arp-cache

Syntax

dhcp-bindings

Mode

TSR options

Description

Enable display of DHCP bindings in tech support report.

Example

dhcp-bindings

Syntax

no dhcp-bindings

Mode

TSR options

Description

Disable display of DHCP bindings in tech support report.

Example

no dhcp-bindings

Syntax

ike-info

Mode

TSR options

Description

Enable display of IKE information in tech support report.

Example

```
ike-info
```

Syntax

```
no ike-info
```

Mode

TSR options

Description

Disable display of IKE information in tech support report.

Example

```
no ike-info
```

Syntax

```
wireless diagnostics
```

Mode

TSR options

Description

Enable display of wireless diagnostics in tech support report.

Example

```
wireless diagnostics
```

Syntax

```
no wireless diagnostics
```

Mode

TSR options

Description

Disable display of wireless diagnostics in tech support report.

Example

```
no wireless diagnostics
```

Syntax

```
users { current | detail | inactive }
```

Mode

TSR options

Description

Enable display of users in tech support report.

Options

- current*** Current users.
- detail*** Detail of users.
- inactive*** Include inactive of users.

Example

```
users current
```

Syntax

```
no users { current | detail | inactive }
```

Mode

TSR options

Description

Disable display of users in tech support report.

Options

- current*** Current users.
- detail*** Detail of users.
- inactive*** Include inactive of users.

Example

```
no users current
```

Syntax

```
ip-stack-info
```

Mode

TSR options

Description

Enable display of IP stack info in tech support report.

Example

```
ip-stack-info
```

Syntax

```
no ip-stack-info
```

Mode

TSR options

Description

Disable display of IP stack info in tech support report.

Example

no ip-stack-info

Syntax

dns-proxy-cache

Mode

TSR options

Description

Enable display of DNS proxy cache info in tech support report.

Example

dns-proxy-cache

Syntax

no dns-proxy-cache

Mode

TSR options

Description

Disable display of DNS proxy cache info in tech support report.

Example

no dns-proxy-cache

Syntax

debug-info

Mode

TSR options

Description

Enable display of debug info in tech support report.

Example

debug-info

Syntax

no debug-info

Mode

TSR options

Description

Disable display of debug info in tech support report.

Example

no debug-info

Syntax

user-name

Mode

TSR options

Description

Enable display of user name in tech support report.

Example

user-name

Syntax

no user-name

Mode

TSR options

Description

Disable display of user name in tech support report.

Example

no user-name

Syntax

ipv6 ndp

Mode

TSR options

Description

Enable display of IPv6 NDP in tech support report.

Example

ipv6 ndp

Syntax

no ipv6 ndp

Mode

TSR options

Description

Disable display of IPv6 NDP in tech support report.

Example

no ipv6 ndp

Syntax

ipv6 dhcp

Mode

TSR options

Description

Enable display of IPv6 DHCP in tech support report.

Example

```
ipv6 dhcp
```

Syntax

```
no ipv6 dhcp
```

Mode

TSR options

Description

Disable display of IPv6 DHCP in tech support report.

Example

```
no ipv6 dhcp
```

Syntax

```
geo-ip-cache
```

Mode

TSR options

Description

Enable display of geo-ip/botnet cache in report in tech support report.

Example

```
geo-ip-cache
```

Syntax

```
no geo-ip-cache
```

Mode

TSR options

Description

Disable display of geo-ip/botnet cache in report in tech support report.

Example

```
no geo-ip-cache
```

Syntax

```
extra-routing
```

Mode

TSR options

Description

Enable display of additional routing commands output in tech support report.

Example

```
extra-routing
```

Syntax

```
no extra-routing
```

Mode

TSR options

Description

Disable display of additional routing commands output in tech support report.

Example

```
no extra-routing
```

Syntax

```
atp-cache
```

Mode

TSR options

Description

Enable display of Capture ATP cache in tech support report.

Example

```
atp-cache
```

Syntax

```
no atp-cache
```

Mode

TSR options

Description

Disable display of Capture ATP cache in tech support report.

Example

```
no atp-cache
```

Syntax

```
vendor-oui
```

Mode

TSR options

Description

Enable display of vendor name resolution in tech support report.

Example

vendor-oui

Syntax

no vendor-oui

Mode

TSR options

Description

Disable display of vendor name resolution in tech support report.

Example

no vendor-oui

Syntax

ip-report

Mode

TSR options

Description

Enable display of IP report in tech support report.

Example

ip-report

Syntax

no ip-report

Mode

TSR options

Description

Disable display of IP report in tech support report.

Example

no ip-report

Syntax

application-signature

Mode

TSR options

Description

Enable display of application signature in tech support report.

Example

application-signature

Syntax

no application-signature

Mode

TSR options

Description

Disable display of application signature in tech support report.

Example

no application-signature

Syntax

abr-entries

Mode

TSR options

Description

Enable display of ABR entries in tech support report.

Example

abr-entries

Syntax

no abr-entries

Mode

TSR options

Description

Disable display of ABR entries in tech support report.

Example

no abr-entries

Syntax

secured-crash-analysis

Mode

TSR options

Description

Enable automatic report secure crash analysis.

Example

secured-crash-analysis

Syntax

no secured-crash-analysis

Mode

TSR options

Description

Disable automatic report secure crash analysis.

Example

no secured-crash-analysis

Syntax

secure-backup [interval <UINT32>]

Mode

TSR options

Description

Enable periodic secure backup of diagnostics report to MySonicwall.

Options

- interval*** Specify backup interval.
- <UINT32>*** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

secure-backup

Syntax

no secure-backup

Mode

TSR options

Description

Disable periodic secure backup of diagnostics report to MySonicwall.

Example

no secure-backup

Syntax

csc-report-time-interval <UINT32>

Mode

TSR options

Description

Set csc reporting time interval (minutes).

Options

- <UINT32>*** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
csc-report-time-interval 20
```

Syntax

```
no csc-report-time-interval
```

Mode

TSR options

Description

Clear csc reporting time interval.

Example

```
no csc-report-time-interval
```

Syntax

```
send-raw-flow-data
```

Mode

TSR options

Description

Enable include raw flow table data entries when sending diagnostic report.

Example

```
send-raw-flow-data
```

Syntax

```
no send-raw-flow-data
```

Mode

TSR options

Description

Disable include raw flow table data entries when sending diagnostic report.

Example

```
no send-raw-flow-data
```

Syntax

```
no packet-replay-file
```

Mode

Packet Replay

Description

Delete the packet replay file.

Example

no packet-replay-file

Syntax

packet-replay

Mode

Config

Description

Enter packet replay configuration mode.

Example

packet-replay

Syntax

replay action-val dest-addr-one <IPV4_HOST> dest-prefix-one <UINT32> dest-iface-one <UINT32> new-dest-flag-one <UINT32> new-dest-addr-one <IPV4_HOST> dest-addr-two <IPV4_HOST> dest-prefix-two <UINT32> dest-iface-two <UINT32> new-dest-flag-two <UINT32> new-dest-addr-two <IPV4_HOST>

Mode

Packet Replay

Description

Replay the pcap file.

Options

<i>dest-addr-one</i>	Enter Destination Address One
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>dest-prefix-one</i>	Enter Destination Prefix One
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>dest-iface-one</i>	Enter Destination Interface One
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>new-dest-flag-one</i>	Enter Destination Flag One
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>new-dest-addr-one</i>	Enter New Destination Address One
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>dest-addr-two</i>	Enter Destination Address Two
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>dest-prefix-two</i>	Enter Destination Prefix Two
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>dest-iface-two</i>	Enter Destination Interface Two
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>new-dest-flag-two</i>	Enter Destination Flag Two
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>new-dest-addr-two</i>	Enter New Destination Address Two
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

replay action-val dest-addr-one 1.1.1.1 dest-prefix-one 32 dest-iface-one 2 new-dest-flag-one 0 new-dest-addr-one 0.0.0.0 dest-addr-two 2.2.2.2 dest-prefix-two 32 dest-iface-two 4 new-dest-flag-two 0 new-dest-addr-two 0.0.0.0

Syntax

individual-replay action-val packet-replay-mode <UINT32> dest-iface <UINT32> packet-id <UINT32> flow-id <UINT32> timestamp <UINT32>

Mode

Packet Replay

Description

Individual Packet Replay.

Options

packet-replay-mode	Enter Packet Replay Mode.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
dest-iface	Enter Recieving Interface.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
packet-id	Enter Packet ID.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
flow-id	Enter flow id.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
timestamp	Enter timestamp.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

individual-replay action-val packet-replay-mode 0 dest-iface 1 packet-id 2 flow-id 0 timestamp 0

Syntax

replay-mac action-val mac-addr-one <MAC> rec-iface-one <UINT32> mac-addr-two <MAC> rec-iface-two <UINT32>

Mode

Packet Replay

Description

Replay the pcap file with MAC Address.

Options

mac-addr-one	Enter Mac Address One
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
rec-iface-one	Enter Receiving interface One.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
mac-addr-two	Enter Mac Address Two
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
rec-iface-two	Enter Receiving interface Two.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

replay-mac action-val mac-addr-one AA:AA:AA:AA:AA:AA rec-iface-one 2 mac-addr-two BB:BB:BB:BB:BB:BB rec-iface-two 3

Syntax

clear packets

Mode

Description

Clear the replayed packets.

Example

```
clear packets
```

Syntax

```
refresh packets
```

Mode

Description

Refresh the replayed packets.

Example

```
refresh packets
```

Syntax

```
packet-crafting-udp action-val dest-iface <UINT32> dest-mac <MAC> src-mac <MAC> ether-type <UINT32> ip-addr-type <UINT32> src-addr <IPV4_HOST> dest-addr <IPV4_HOST> ttl-val <UINT32> src-port <UINT32> dst-port <UINT32> [ payload <WORD> ]
```

Mode

Description

Packet Crafting UDP.

Options

dest-iface	Enter destination interface
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
dest-mac	Enter destination Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
src-mac	Enter source Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
ether-type	Enter ether type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
ip-addr-type	Enter IP address type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
src-addr	Enter Source Address
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168
dest-addr	Enter Destination Address
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168
ttl-val	Enter TTL Value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
src-port	Enter Source Port
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123

dst-port	Enter Destination Port
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
payload	Enter Payload
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: abc

Example

```
packet-crafting-udp action-val dest-iface 2 dest-mac AA:AA:AA:AA:AA:AA src-mac CC:CC:CC:CC:CC:CC ether-type 0 ip-addr-type 0
src-addr 1.1.1.1 dest-addr 2.2.2.2 ttl-val 30 src-port 22 dst-port 32 payload ABCDEF
```

Syntax

```
packet-crafting-icmp action-val dest-iface <UINT32> dest-mac <MAC> src-mac <MAC> ether-type <UINT32> ip-addr-type <UINT32>
src-addr <IPV4_HOST> dest-addr <IPV4_HOST> ttl-val <UINT32> icmp-type <UINT32> id-val <UINT32> sequence-val <UINT32> [ payload
<WORD> ]
```

Mode

Packet Replay

Description

Packet Crafting ICMP.

Options

dest-iface	Enter destination interface
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
dest-mac	Enter destination Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
src-mac	Enter source Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
ether-type	Enter ether type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
ip-addr-type	Enter IP address type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
src-addr	Enter Source Address
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
dest-addr	Enter Destination Address
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
ttl-val	Enter TTL Value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
icmp-type	Enter ICMP Type value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
id-val	Enter ID value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
sequence-val	Enter Sequence Value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
payload	Enter Payload
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: abc

Example

```
packet-crafting-icmp action-val dest-iface 2 dest-mac AA:AA:AA:AA:AA:AA src-mac CC:CC:CC:CC:CC:CC ether-type 1 ip-addr-type 0
src-addr 1.1.1.1 dest-addr 2.2.2.2 ttl-val 30 icmp-type 0 id-val 1 sequence-val 1 payload ABCDEF
```

Syntax

```
packet-crafting-igmp action-val dest-iface <UINT32> dest-mac <MAC> src-mac <MAC> ether-type <UINT32> ip-addr-type <UINT32>
src-addr <IPV4_HOST> dest-addr <IPV4_HOST> ttl-val <UINT32> igmp-type <UINT32> max-resp <UINT32> group-addr <IPV4_HOST> [
payload <WORD> ]
```

Mode

Packet Replay

Description

Packet Crafting IGMP.

Options

dest-iface	Enter destination interface
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
dest-mac	Enter destination Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
src-mac	Enter source Mac Address
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: 00:0C:F1:56:98:AD
ether-type	Enter ether type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
ip-addr-type	Enter IP address type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
src-addr	Enter Source Address
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
dest-addr	Enter Destination Address
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
ttl-val	Enter TTL Value
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
igmp-type	Enter IGMP Type
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
max-resp	Enter Maximum response
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
group-addr	Enter Group Address
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
payload	Enter Payload
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: abc

Example

```
packet-crafting-igmp action-val dest-iface 2 dest-mac AA:AA:AA:AA:AA:AA src-mac CC:CC:CC:CC:CC:CC ether-type 2 ip-addr-type 0
src-addr 1.1.1.1 dest-addr 2.2.2.2 ttl-val 30 igmp-type 0 max-resp 1 group-addr 3.3.3.3 payload ABCDEF
```

Syntax

```
packet-crafting-buffer action-val dest-iface <UINT32> payload <WORD>
```

Mode

Packet Replay

Description

Packet Crafting buffer.

Options

dest-iface	Enter destination interface
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH.

	Example: 123
payload	Enter Payload
<WORD>	Word in the form: WORD or \"QUOTED STRING\".
	Example: abc

Example

```
packet-crafting-buffer action-val dest-iface 1 payload ABCDEF01
```

Syntax

```
diag show ipnet { interfaces | ndp | route | sockets | statistic | tcp-statistic }
```

Mode

All Modes

Description

Show IPNET status and configuration.

Options

- interfaces** Show IPNET interfaces status.
- ndp** Show IPNET NDP table.
- route** Show IPNET routing table.
- sockets** Show the state of all IPNET sockets.
- statistic** Show IPNET statistic.
- tcp-statistic** Show IPNET tcp statistic.

Example

```
diag show ipnet interfaces
diag show ipnet sockets
diag show ipnet route
diag show ipnet ndp
diag show ipnet statistic
diag show ipnet tcp-statistic
```

Syntax

```
diag show advanced [ anti-spam | arp | backend | base | cta-report | dhcp | diagnostics | dial-up | dns | dns-proxy | dns-security | dpi-ssl | encryption | firewall | flow-reporting | fqdn-dyn-addr-obj | geoip-location-service | high-availability | management | network | network-fo-lb | pppoe | preference | security-service | ssl-vpn | trace-log | user-authentication | voip | vpn | watchdog | wireless | zero-touch ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show advanced diag configuration.

Options

- anti-spam** Anti-Spam settings.
- arp** ARP settings.
- backend** Backend Server settings.
- base** Advanced diag global settings.

<i>cta-report</i>	Advanced diag capture threat assessment report configuration settings.
<i>dhcp</i>	DHCP settings.
<i>diagnostics</i>	Diagnostics settings.
<i>dial-up</i>	Dial-up settings.
<i>dns</i>	DNS settings.
<i>dns-proxy</i>	DNS proxy settings.
<i>dns-security</i>	DNS Security settings.
<i>dpi-ssl</i>	DPI-SSL settings.
<i>encryption</i>	Encryption settings
<i>firewall</i>	Firewall settings.
<i>flow-reporting</i>	Flow Reporting settings.
<i>fqdn-dyn-addr-obj</i>	Advanced diag fqdn address object settings.
<i>geoip-location-service</i>	GeoIP/Location Service settings.
<i>high-availability</i>	High Availability settings.
<i>management</i>	Management settings.
<i>network</i>	Network settings.
<i>network-fs-lb</i>	Network Failover and Load Balancing settings.
<i>pppoe</i>	PPPoE settings.
<i>preference</i>	Preference Conversion settings.
<i>security-service</i>	Security Services settings.
<i>ssl-vpn</i>	SSL-VPN settings.
<i>trace-log</i>	Trace log settings.
<i>user-authentication</i>	User Authentication settings.
<i>voip</i>	VoIP settings.
<i>vpn</i>	VPN settings.
<i>watchdog</i>	Watchdog settings.
<i>wireless</i>	Wireless settings.
<i>zero-touch</i>	Zero Touch settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
diag show advanced arp
```



Syntax

```
show packet-monitor [ packet <UINT32> | packets | statistics ]
```

Mode

All Modes

Description

Show packet monitor configuration.

Options

packet Show one captured packet with detail.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

packets Show all captured packets in list.

statistics Show packet monitor statistics.

Example

```
show packet-monitor
```

Syntax

```
show tech-support-report [ access-rules | active-utm | address-objects | anti-spam | anti-virus | arp-cache | backups | cache-check | content-filtering | db-trace | dhcp-client | dhcp-network-disc | dhcp-persistence | dhcp-relay | dhcp-server | dhcp-serverstat | diag | dns-proxy-cache | dpi-ssl { { client | server } } | dynamic-dns | ethernet | flight-data-recorder | gateway-anti-virus | guest-profile-objects | h323 | high-availability | interfaces | intrusion-detection-prevention | ip-helper | ip-reassembly | ipsec | l2tp-client | l2tp-server | ldap | license | management | mirror-state | modem | multicast | nat-policies | network | objects | options | pki | port-counters | port-remap-stats | port-status | pppoe-client | pptp-client | pref-stats | product | qos | radius | redirector-status [ list | statistics | summary | verbose ] | route-policies | routes | rtsp | schedule-objects | sd-wan | service-objects | session-pipes | single-sign-on [ full | statistics | status | summary ] | sip | snmp | sonicpoint | ssl-control | stateful-stats | stateful-sync | status | time | timers | update | user-objects | users-guest-users | users-local-groups | users-local-users | users-settings [ debug ] | users-status [ full | list | summary ] | inactive ] [ debug ] | wan-load-balancing | wire-mode | wireless | wlan-zone | zone-objects ]
```

Mode

All Modes

Description

Display basic system status and information.

Options

- access-rules** Access rules technical support report.
- active-utm** Active-active UTM technical support report.
- address-objects** Address object table technical support report.
- anti-spam** Anti-spam technical support report.
- anti-virus** AV technical support report.
- arp-cache** ARP cache technical support report.
- backups** Backup support report.
- cache-check** Cache check technical support report.
- content-filtering** CFL technical support report.
- db-trace** DB trace dump technical support report.

<i>dhcp-client</i>	DHCP client technical support report.
<i>dhcp-network-disc</i>	DHCP network discovery technical support report.
<i>dhcp-persistence</i>	DHCP persistence technical support report.
<i>dhcp-relay</i>	DHCP relay technical support report.
<i>dhcp-server</i>	DHCP server technical support report.
<i>dhcp-serverstat</i>	DHCP server stats technical support report.
<i>diag</i>	Diagnostics technical support report.
<i>dns-proxy-cache</i>	DNS Proxy Cache Technical Support Report.
<i>dpi-ssl</i>	DPI SSL technical support report.
<i>client</i>	DPI SSL client technical support report.
<i>server</i>	DPI SSL server technical support report.
<i>dynamic-dns</i>	Dynamic dns technical support report.
<i>ethernet</i>	Ethernet technical support report.
<i>flight-data-recorder</i>	Flight data recorder technical support report.
<i>gateway-anti-virus</i>	Global anti-virus technical support report.
<i>guest-profile-objects</i>	Guest profile objects technical support report.
<i>h323</i>	H.323 technical support report.
<i>high-availability</i>	HA technical support report.
<i>interfaces</i>	Interfaces technical support report.
<i>intrusion-detection-prevention</i>	IDP technical support report.
<i>ip-helper</i>	IP helper technical support report.
<i>ip-reassembly</i>	IP fragment reassembly technical support report.
<i>ipsec</i>	IPSec technical support report.
<i>l2tp-client</i>	L2tp client technical support report.
<i>l2tp-server</i>	L2tp server technical support report.
<i>ldap</i>	LDAP technical support report.
<i>license</i>	License technical support report.
<i>management</i>	Management technical support report.
<i>mirror-state</i>	Flash prefs mirror state technical support report.
<i>modem</i>	Modem technical support report.
<i>multicast</i>	Mcast igmp config technical support report.
<i>nat-policies</i>	NAT policies technical support report.
<i>network</i>	Network technical support report.
<i>objects</i>	Network objects technical support report.

<i>options</i>	Options of technical support report.
<i>pki</i>	PKI technical support report.
<i>port-counters</i>	Port counters technical support report.
<i>port-remap-stats</i>	Port remap technical support report.
<i>port-status</i>	Port status technical support report.
<i>pppoe-client</i>	PPPoE client technical support report.
<i>pptp-client</i>	PPTP client technical support report.
<i>pref-stats</i>	Flash prefs load/save technical support report.
<i>product</i>	Product technical support report.
<i>qos</i>	QOS technical support report.
<i>radius</i>	Radius technical support report.
<i>redirector-status</i>	HTTP/HTTPS redirector status technical support report.
<i>list</i>	Include a list of redirected users.
<i>statistics</i>	Show statistics counters only.
<i>summary</i>	Show an overall summary only.
<i>verbose</i>	Show detailed information.
<i>route-policies</i>	Detailed route policy table technical support report.
<i>routes</i>	Routing table.
<i>rtsp</i>	RTSP technical support report.
<i>schedule-objects</i>	Service object table technical support report.
<i>sd-wan</i>	SD-WAN technical support report.
<i>service-objects</i>	Service object table technical support report.
<i>session-pipes</i>	Session pipes support report.
<i>single-sign-on</i>	Single sign on technical support report.
<i>full</i>	Show full information including a (possibly lengthy) list of SSO failures.
<i>statistics</i>	Show only the SSO statistics.
<i>status</i>	Show only the SSO status information.
<i>summary</i>	Show an overall summary only.
<i>sip</i>	SIP technical support report.
<i>snmp</i>	Snmp technical support report.
<i>sonicpoint</i>	Sonicpoint technical support report.
<i>ssl-control</i>	SSL control technical support report.
<i>stateful-stats</i>	Stateful stats technical support report.

<i>stateful-sync</i>	Stateful sync technical support report.
<i>status</i>	Status technical support report.
<i>time</i>	Time technical support report.
<i>timers</i>	Timers technical support report.
<i>update</i>	Update technical support report.
<i>user-objects</i>	User object table technical support report.
<i>users-guest-users</i>	Guest User Accounts Technical Support Report.
<i>users-local-groups</i>	Local User Groups Technical Support Report.
<i>users-local-users</i>	Local User Accounts Technical Support Report.
<i>users-settings</i>	Users Settings Technical Support Report.
<i>debug</i>	Include additional debug information.
<i>users-status</i>	Users Status Technical Support Report.
<i>full</i>	Show full detail of each user.
<i>list</i>	Include a terse list of connected users.
<i>summary</i>	Show an overall summary only.
<i>inactive</i>	Include a list of inactive users.
<i>debug</i>	Include additional debug information.
<i>wan-load-balancing</i>	WLB technical support report.
<i>wire-mode</i>	Wire mode technical support report.
<i>wireless</i>	Wireless technical support report.
<i>wlan-zone</i>	Wlan zone technical support report.
<i>zone-objects</i>	Zone object table technical support report.

Example

show tech-support-report

Syntax

auth

Mode

DBG-SETTING

Description

Authentication debug setting.

Example

auth

Syntax

tsa <UINT16>

Mode

AUTH

Description

Set TSA debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

tsa 5

Syntax

cia <UINT16>

Mode

AUTH

Description

Set CIA debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

cia 5

Syntax

rad-acct <UINT16>

Mode

AUTH

Description

Set Radius account debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

rad-acct 5

Syntax

sso-api <UINT16>

Mode

AUTH

Description

Set SSO api debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

sso-api 5

Syntax

radius

Mode

AUTH

Description

Turn on radius authentication debugging.

Example

radius

Syntax

no radius

Mode

AUTH

Description

Turn off radius auth debug.

Example

no radius

Syntax

ldap { all | args | ber | client | conns | daemon | filter | namerresolve | packets | parse | pktdump | relay | socketdump | tool | toolverbose | trace }

Mode

AUTH

Description

different ldap debug option.

Options

all	enable all ldap debug
args	enable ldap arguments debug
ber	enable ldap ber debug
client	enable ldap client debug
conns	enable ldap conns debug

<i>daemon</i>	enable ldap daemon debug
<i>filter</i>	enable ldap filter debug
<i>nameresolve</i>	enable ldap nameresolve debug
<i>packets</i>	enable ldap packets debug
<i>parse</i>	enable ldap parse debug
<i>pktdump</i>	enable ldap pktdump debug
<i>relay</i>	enable ldap relay debug
<i>socketdump</i>	enable ldap socketdump debug
<i>tool</i>	enable ldap tool debug
<i>toolverbose</i>	enable ldap toolverbose debug
<i>trace</i>	enable ldap trace debug

Example

```
ldap client
ldap daemon
ldap tool
ldap relay
ldap trace
ldap packets
ldap args
ldap conns
ldap ber
ldap filter
ldap parse
ldap toolverbose
ldap nameresolve
ldap pktdump
ldap socketdump
ldap all
```

Syntax

```
no ldap { all | args | ber | client | conns | daemon | filter | nameresolve | packets | parse | pktdump | relay | socketdump |
tool | toolverbose | trace }
```

Mode

AUTH

Description

different ldap debug option.

Options

<i>all</i>	turn off all ldap debug
<i>args</i>	turn off ldap arguments debug
<i>ber</i>	turn off ldap ber debug
<i>client</i>	turn off ldap client debug
<i>conns</i>	turn off ldap conns debug
<i>daemon</i>	turn off ldap daemon debug
<i>filter</i>	turn off ldap filter debug

<i>nameresolve</i>	turn off ldap nameresolve debug
<i>packets</i>	turn off ldap packets debug
<i>parse</i>	turn off ldap parse debug
<i>pktdump</i>	turn off ldap pktdump debug
<i>relay</i>	turn off ldap relay debug
<i>socketdump</i>	turn off ldap socketdump debug
<i>tool</i>	turn off ldap tool debug
<i>toolverbose</i>	turn off ldap toolverbose debug
<i>trace</i>	turn off ldap trace debug

Example

```
no ldap client
no ldap daemon
no ldap tool
no ldap relay
no ldap trace
no ldap packets
no ldap args
no ldap conns
no ldap ber
no ldap filter
no ldap parse
no ldap toolverbose
no ldap nameresolve
no ldap pktdump
no ldap socketdump
no ldap all
```

Syntax

```
tacas
```

Mode

AUTH

Description

Turn on tacas debugging.

Example

```
tacas
```

Syntax

```
no tacas
```

Mode

AUTH

Description

Turn off tacas debug.

Example

```
no tacas
```

Syntax

```
user
```

Mode

DBG-SETTING

Description

User debug setting.

Example

```
user
```

Syntax

```
auth-level <UINT16>
```

Mode

USER

Description

Set user auth debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
auth-level 5
```

Syntax

```
ha-level <UINT16>
```

Mode

USER

Description

Set user ha debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
ha-level 5
```

Syntax

```
conn-level <UINT16>
```

Mode

USER

Description

Set user connection debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
conn-level 5
```

Syntax

```
ip-level <UINT16>
```

Mode

USER

Description

Set user ip debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
ip-level 5
```

Syntax

```
ha
```

Mode

DBG-SETTING

Description

HA debug setting.

Example

```
ha
```

Syntax

```
haf
```

Mode

HA

Description

Enable ha filter.

Example

```
haf
```

Syntax

```
no haf
```

Mode

HA

Description

Disable ha filter.

Example

```
no haf
```

Syntax

```
haf-src <IPV4_HOST>
```

Mode

HA

Description

Set ha filter src IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
haf-src 1.1.1.1
```

Syntax

```
haf-dst <IPV4_HOST>
```

Mode

HA

Description

Set ha filter dst IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
haf-dst 1.1.1.1
```

Syntax

```
module { all | arp | cgi | encryption | event | http | incomingpkt | ipv6 | monitoring | outgoingpkt | policy | recvpkt |  
statemachine | svrrpgrpowner | svrrppkt | svrrpstatemachine | taskctx | timer }
```

Mode

HA

Description

ha debug option.

Options

<i>all</i>	enable all debug
<i>arp</i>	enable ha arp debug
<i>cgi</i>	enable ha cgi debug
<i>encryption</i>	enable ha encryption debug
<i>event</i>	enable ha event debug
<i>http</i>	enable ha http debug
<i>incomingpkt</i>	enable ha incoming pkt debug
<i>ipv6</i>	enable ha ipv6 debug
<i>monitoring</i>	enable ha monitoring debug
<i>outgoingpkt</i>	enable ha outgoingpkt debug
<i>policy</i>	enable ha policy debug
<i>recvpkt</i>	enable ha receiving packet debug
<i>statemachine</i>	enable ha statemachine debug
<i>svrrpgrpowner</i>	enable ha svrrp group owner debug
<i>svrrppkt</i>	enable ha svrrp packet debug
<i>svrrpstatemachine</i>	enable ha svrrp state machine debug
<i>taskctx</i>	enable ha task context debug
<i>timer</i>	enable ha timer debug

Example

```
module statemachine
module event
module recvpkt
module incomingpkt
module outgoingpkt
module cgi
module policy
module timer
module http
module monitoring
module arp
module svrrppkt
module svrrpstatemachine
module svrrpgrpowner
module ipv6
module taskctx
module encryption
module all
```

Syntax

```
no module { all | arp | cgi | encryption | event | http | incomingpkt | ipv6 | monitoring | outgoingpkt | policy | recvpkt |
statemachine | svrrpgrpowner | svrrppkt | svrrpstatemachine | taskctx | timer }
```

Mode

HA

Description

ha debug option.

Options

<i>all</i>	disable all debug
<i>arp</i>	disable ha arp debug
<i>cgi</i>	disable ha cgi debug
<i>encryption</i>	disable ha encryption debug
<i>event</i>	disable ha event debug
<i>http</i>	disable ha http debug
<i>incomingpkt</i>	disable ha incoming pkt debug
<i>ipv6</i>	disable ha ipv6 debug
<i>monitoring</i>	disable ha monitoring debug
<i>outgoingpkt</i>	disable ha outgoingpkt debug
<i>policy</i>	disable ha policy debug
<i>recvpkt</i>	disable ha receiving packet debug
<i>statemachine</i>	disable ha statemachine debug
<i>svrrpgrpowner</i>	disable ha svrrp group owner debug
<i>svrrppkt</i>	disable ha svrrp packet debug
<i>svrrpstatemachine</i>	disable ha svrrp state machine debug
<i>taskctx</i>	disable ha task context debug
<i>timer</i>	disable ha timer debug

Example

```
module statemachine
module event
module recvpkt
module incomingpkt
module outgoingpkt
module cgi
module policy
module timer
module http
module monitoring
module arp
module svrrppkt
module svrrpstatemachine
module svrrpgrpowner
module ipv6
module taskctx
module encryption
module all
```

Syntax

```
vpn
```

Mode

DBG-SETTING

Description

VPN debug setting.

Example

vpn

Syntax

cfg <UINT16>

Mode

vpn

Description

Set vpn config debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

cfg 5

Syntax

gen <UINT16>

Mode

vpn

Description

Set vpn general debug level(0-10).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

gen 5

Syntax

addnewln

Mode

vpn

Description

Turn on add newline.

Example

addnewln

Syntax

no addnewln

Mode

vpn

Description

Turn off addnewln.

Example

no addnewln

Syntax

matchlevel

Mode

vpn

Description

Turn on match level.

Example

matchlevel

Syntax

no matchlevel

Mode

vpn

Description

Turn off matchlevel.

Example

no matchlevel

Syntax

vpn { activestate | autorule | bitmap | bladedisplay | config | gms | iphcfg | look_up | manualkey | natpol | policy |
prisecgw | routeadv | snmp | spd | tunnelif | vpn_ha }

Mode

vpn

Description

specify vpn submodule.

Options

activestate enable vpn activestate

autorule enable vpn autorule

bitmap enable vpn bitmap

bladedisplay enable vpn bladedisplay

config enable vpn config

<i>gms</i>	enable vpn gms
<i>iphcfg</i>	enable vpn iphcfg
<i>look_up</i>	enable vpn look_up
<i>manualkey</i>	enable vpn manualkey
<i>natpol</i>	enable vpn natpol
<i>policy</i>	enable vpn policy
<i>prisecgw</i>	enable vpn prisecgw
<i>routeadv</i>	enable vpn routeadv
<i>snmp</i>	enable vpn snmp
<i>spd</i>	enable vpn spd
<i>tunnelif</i>	enable vpn tunnelif
<i>vpn_ha</i>	enable vpn vpn_ha

Example

```
vpn policy
vpn bitmap
vpn autorule
vpn routeadv
vpn snmp
vpn gms
vpn manualkey
vpn tunnelif
vpn natpol
vpn iphcfg
vpn prisecgw
vpn config
vpn spd
vpn vpn_ha
vpn activestate
vpn look_up
vpn bladedisplay
```

Syntax

```
no vpn { activestate | autorule | bitmap | bladedisplay | config | gms | iphcfg | look_up | manualkey | natpol | policy |
prisecgw | routeadv | snmp | spd | tunnelif | vpn_ha }
```

Mode

vpn

Description

specify vpn submodule.

Options

<i>activestate</i>	disable vpn activestate
<i>autorule</i>	disable vpn autorule
<i>bitmap</i>	disable vpn bitmap
<i>bladedisplay</i>	disable vpn bladedisplay
<i>config</i>	disable vpn config
<i>gms</i>	disable vpn gms

<i>iphcfg</i>	disable vpn iphcfg
<i>look_up</i>	disable vpn look_up
<i>manualkey</i>	disable vpn manualkey
<i>natpol</i>	disable vpn natpol
<i>policy</i>	disable vpn policy
<i>prisecgw</i>	disable vpn prisecgw
<i>routeadv</i>	disable vpn routeadv
<i>snmp</i>	disable vpn snmp
<i>spd</i>	disable vpn spd
<i>tunnelif</i>	disable vpn tunnelif
<i>vpn_ha</i>	disable vpn vpn_ha

Example

```
no vpn policy
no vpn bitmap
no vpn autorule
no vpn routeadv
no vpn snmp
no vpn gms
no vpn manualkey
no vpn tunnelif
no vpn natpol
no vpn iphcfg
no vpn prisecgw
no vpn config
no vpn spd
no vpn vpn_ha
no vpn activestate
no vpn look_up
no vpn bladedisplay
```

Syntax

```
ipsec { crypt | frag | mcast | nbns | packetfwd | replay | selcheck | stats | traffic }
```

Mode

vpn

Description

specify ipsec submodule.

Options

<i>crypt</i>	enable ipsec crypt
<i>frag</i>	enable ipsec frag
<i>mcast</i>	enable ipsec mcast
<i>nbns</i>	enable ipsec nbns
<i>packetfwd</i>	enable ipsec packetfwd
<i>replay</i>	enable ipsec replay
<i>selcheck</i>	enable ipsec selcheck
<i>stats</i>	enable ipsec stats

traffic enable ipsec traffic

Example

```
ipsec traffic
ipsec frag
ipsec mcast
ipsec stats
ipsec nbns
ipsec replay
ipsec crypt
ipsec selcheck
ipsec packetfwd
```

Syntax

```
no ipsec { crypt | frag | mcast | nbns | packetfwd | replay | selcheck | stats | traffic }
```

Mode

vpn

Description

specify ipsec submodule.

Options

crypt	disable ipsec crypt
frag	disable ipsec frag
mcast	disable ipsec mcast
nbns	disable ipsec nbns
packetfwd	disable ipsec packetfwd
replay	disable ipsec replay
selcheck	disable ipsec selcheck
stats	disable ipsec stats
traffic	disable ipsec traffic

Example

```
no ipsec traffic
no ipsec frag
no ipsec mcast
no ipsec stats
no ipsec nbns
no ipsec replay
no ipsec crypt
no ipsec selcheck
no ipsec packetfwd
```

Syntax

```
ike { autoprov | blade | dhcprelay | dpd | groupvpn | handle | ikekeys | ikev2 | keepalive | l2tp | mempool | nattrav | negn | obsp | packet | phase1 | phase2 | pki | spd | xauth }
```

Mode

vpn

Description

specify ike submodule.

Options

<i>autoprov</i>	enable ike autoprov
<i>blade</i>	enable ike blade
<i>dhcprelay</i>	enable ike dhcprelay
<i>dpd</i>	enable ike dpd
<i>groupvpn</i>	enable ike groupvpn
<i>handle</i>	enable ike handle
<i>ikekeys</i>	enable ike keys
<i>ikev2</i>	enable ike ikev2
<i>keepalive</i>	enable ike keepalive
<i>l2tp</i>	enable ike l2tp
<i>mempool</i>	enable ike mempool
<i>nattrav</i>	enable ike nat traverse
<i>negn</i>	enable ike negn
<i>ocsp</i>	enable ike ocsp
<i>packet</i>	enable ike packet
<i>phase1</i>	enable ike phase1
<i>phase2</i>	enable ike phase2
<i>pki</i>	enable ike pki
<i>spd</i>	enable ike spd
<i>xauth</i>	enable ike xauth

Example

```
ike dpd
ike keepalive
```

Syntax

```
no ike { autoprov | blade | dhcprelay | dpd | groupvpn | handle | ikekeys | ikev2 | keepalive | l2tp | mempool | nattrav |
negn | ocsp | packet | phase1 | phase2 | pki | spd | xauth }
```

Mode

vpn

Description

different module debug option.

Options

<i>autoprov</i>	disable ike autoprov

<i>blade</i>	disable ike blade
<i>dhcprelay</i>	disable ike dhcprelay
<i>dpd</i>	disable ike dpd
<i>groupvpn</i>	disable ike groupvpn
<i>handle</i>	disable ike handle
<i>ikekeys</i>	disable ike keys
<i>ikev2</i>	disable ike ikev2
<i>keepalive</i>	disable ike keepalive
<i>l2tp</i>	disable ike l2tp
<i>mempool</i>	disable ike mempool
<i>nattrav</i>	disable ike nat traverse
<i>negn</i>	disable ike negn
<i>ocsp</i>	disable ike ocsp
<i>packet</i>	disable ike packet
<i>phase1</i>	disable ike phase1
<i>phase2</i>	disable ike phase2
<i>pki</i>	disable ike pki
<i>spd</i>	disable ike spd
<i>xauth</i>	disable ike xauth

Example

```
no ike dpd
no ike keepalive
no ike mempool
no ike xauth
no ike autoprov
no ike nattrav
no ike ocsp
no ike dhcprelay
no ike l2tp
no ike phase1
no ike phase2
no ike spd
no ike packet
no ike pki
no ike groupvpn
no ike handle
no ike negn
no ike ikev2
no ike ikekeys
no ike blade
```



Syntax

```
module { ike | ipsec | vpn }
```

Mode

vpn

Description

specify vpn module.

Options

<i>ike</i>	enable module ike debug
<i>ipsec</i>	enable module ipsec debug
<i>vpn</i>	enable module vpn debug

Example

```
module ike
module ipsec
module vpn
```

Syntax

```
no module { ike | ipsec | vpn }
```

Mode

vpn

Description

different module debug option.

Options

<i>ike</i>	turn off module ike debug
<i>ipsec</i>	turn off module ipsec debug
<i>vpn</i>	turn off module vpn debug

Example

```
no module ike
no module ipsec
no module vpn
```

Syntax

```
show dbg [ auth | ha | user | vpn ]
```

Mode

All Modes

Description

Show debug settings.

Options

<i>auth</i>	Show authentication debug settings.
<i>ha</i>	Show ha debug settings.
<i>user</i>	Show user debug settings.
<i>vpn</i>	Show vpn debug settings.

Example

```
show dbg
```

Syntax

```
address-object ipv4 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit IPv4 address object.

Options

uuid	Edit an address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
zone	Address object zone.
<ZONE_NAME>	Zone object name. Example: <i>DMZ</i>

Example

```
address-object ipv4 "Mail Server" host 192.168.168.33 zone DMZ
address-object ipv4 "Web Servers" range 192.168.100.50 192.168.100.60
address-object ipv4 "HR Network" network 192.168.100.0 /24
address-object ipv4 "HR Network" network 192.168.100.0 255.255.255.0
```

Syntax

```
no address-object ipv4 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid	Delete an IPv4 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>

Example

```
no address-object ipv4 "Web Server"
```

Syntax

```
address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit IPv6 address object.

Options

uuid	Edit an IPv6 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
zone	Address object zone.
<ZONE_NAME>	Zone object name. Example: <i>DMZ</i>

Example

```
address-object ipv6 "Mail Server" host fe80::217:c5ff:fec1 zone DMZ
address-object ipv6 "Web Servers" range fe80::217:c5ff:fec1 fe80::217:c5ff:ffff
address-object ipv6 "HR Network" network fe80::217:c5ff:fec1 /64
```

Syntax

```
no address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid	Delete an IPv6 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>

Example

```
no address-object ipv6 "Web Server"
```

Syntax

```
address-object mac [ uuid ] <ADDR_MAC_NAME> [ address <ADDR_MAC> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit MAC address object.

Options

uuid	Edit a MAC address object by UUID.
<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>
address	MAC address.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
zone	Address object zone.
<ZONE_NAME>	Zone object name. Example: <i>DMZ</i>

Example

```
address-object mac "WAP MAC" address 00:09:5B:BD:93:DB
```

Syntax

```
no address-object mac [ uuid ] <ADDR_MAC_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid	Delete a MAC address object by UUID.
<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>

Example

```
no address-object mac "Sales Network Access Point"
```

Syntax

```
address-object fqdn [ uuid ] <ADDR_FQDN_NAME> [ domain <ADDR_FQDN> ] [ zone <ZONE_NAME> ]
```

Mode

Config

Description

Add/edit FQDN address object.

Options

uuid	Edit an FQDN address object by UUID.
<ADDR_FQDN_NAME>	FQDN address object name. Example: <i>www.example.com</i>
domain	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
zone	Address object zone.
<ZONE_NAME>	Zone object name.

Example

```
address-object fqdn Whitelist domain *.google.com
```

Syntax

```
no address-object fqdn [ uuid ] <ADDR_FQDN_NAME>
```

Mode

Config

Description

Delete an address object.

Options

uuid	Delete an FQDN address object by UUID.
<ADDR_FQDN_NAME>	FQDN address object name. Example: <i>www.example.com</i>

Example

```
no address-object fqdn "*.example.com"
```

Syntax

```
no address-objects [ fqdn | host | ipv4 | ipv6 | mac | network | range ]
```

Mode

Config

Description

Delete all custom address objects.

Options

fqdn	Delete all custom FQDN address objects.
host	Delete all custom host address objects.
ipv4	IPV4 address object.
ipv6	IPV6 address object.
mac	Delete all custom MAC address objects.
network	Delete all custom network address objects.
range	Delete all custom range address objects.

Example

```
no address-objects
```

Syntax

```
address-object resolve [ fqdn <ADDR_FQDN_NAME> | mac <ADDR_MAC_NAME> ]
```

Mode

Config

Description

Resolve a specified MAC/FQDN address object or all address objects.

Options

<i>fqdn</i>	Resolve a FQDN address object.
<i><ADDR_FQDN_NAME></i>	FQDN address object name. Example: <i>www.example.com</i>
<i>mac</i>	Resolve a MAC address object.
<i><ADDR_MAC_NAME></i>	MAC address object name. Example: <i>Sales Network Access Point</i>

Example

```
address-object resolve mac "WAP MAC"
address-object resolve fqdn "*.example.com"
address-object resolve
```

Syntax

```
address-object purge [ fqdn <ADDR_FQDN_NAME> | mac <ADDR_MAC_NAME> ]
```

Mode

Config

Description

Purge a specified MAC/FQDN address object or all address objects.

Options

<i>fqdn</i>	Purge a FQDN address object.
<i><ADDR_FQDN_NAME></i>	FQDN address object name. Example: <i>www.example.com</i>
<i>mac</i>	Purge a MAC address object.
<i><ADDR_MAC_NAME></i>	MAC address object name. Example: <i>Sales Network Access Point</i>

Example

```
address-object purge mac "WAP MAC"
address-object purge fqdn "*.example.com"
address-object purge
```

Syntax

```
address-group ipv4 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Add/edit IPv4 address group.

Options

<i>uuid</i>	Edit an IPv4 address group by UUID.
<i><ADDR_GROUP_NAME></i>	Group address object name. Example: <i>Sales Group</i>

Example

```
address-group ipv4 "Corp Web Servers"
```

Syntax

```
no address-group ipv4 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Delete an IPv4 address group.

Options

uuid	Delete an IPv4 address group by UUID.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>

Example

```
no address-group ipv4 "Corp Web Servers"
```

Syntax

```
address-group ipv6 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Add/edit IPv6 address group.

Options

uuid	Delete an IPv6 address group by UUID.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>

Example

```
address-group ipv6 "Corp Web Servers"
```

Syntax

```
no address-group ipv6 [ uuid ] <ADDR_GROUP_NAME>
```

Mode

Config

Description

Delete an IPv4 address group.

Options

uuid	Delete an IPv6 address group by UUID.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>

Example

```
no address-group ipv6 "Corp Web Servers"
```

Syntax

```
no address-groups [ ipv4 | ipv6 ]
```

Mode

Config

Description

Delete all custom address groups.

Options

ipv4 Delete all IPv4 address groups.

ipv6 Delete all IPv6 address groups.

Example

```
no address-groups
```

Syntax

```
uuid <UUID>
```

Mode

Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Address Object

Description

Clear address object UUID.

Example

```
no uuid
```

Syntax

```
name <ADDR_HOST_NETWORK_RANGE_NAME>
```

Mode

Address Object

Description

Set address object name.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

name "Corp E-mail Server"

Syntax

host <ADDR_HOST>

Mode

Address Object

Description

Set address object host.

Options

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

Example

host 10.10.10.10

Syntax

no host

Mode

Address Object

Description

Clear address object host.

Example

no host

Syntax

range <ADDR_BEGIN> <ADDR_END>

Mode

Address Object

Description

Set address object range.

Options

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

```
range 10.10.10.1 10.10.10.10
```

Syntax

```
no range
```

Mode

Address Object

Description

Clear address object range.

Example

```
no range
```

Syntax

```
network <ADDR_NETWORK> <ADDR_MASK>
```

Mode

Address Object

Description

Set address object network.

Options

<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>

Example

```
network 10.10.10.0 255.255.255.0
```

Syntax

```
no network
```

Mode

Address Object

Description

Clear address object network.

Example

```
no network
```

Syntax

```
zone <ZONE_NAME>
```

Mode

Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

zone WAN

Syntax

uuid <UUID>

Mode

MAC Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

MAC Address Object

Description

Clear address object UUID.

Example

no uuid

Syntax

name <ADDR_MAC_NAME>

Mode

MAC Address Object

Description

Set address object name.

Options

<ADDR_MAC_NAME> MAC address object name.
Example: *Sales Network Access Point*

Example

```
name "Corp E-mail Server"
```

Syntax

```
address <ADDR_MAC>
```

Mode

MAC Address Object

Description

Set address object MAC.

Options

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

Example

```
address 00:D0:68:09:4B:2A
```

Syntax

```
no address
```

Mode

MAC Address Object

Description

Clear address object MAC.

Example

```
no address
```

Syntax

```
zone <ZONE_NAME>
```

Mode

MAC Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone WAN
```

Syntax

multi-homed

Mode

MAC Address Object

Description

Enable multi-homed host.

Example

multi-homed

Syntax

no multi-homed

Mode

MAC Address Object

Description

Disable multi-homed host.

Example

no multi-homed

Syntax

uuid <UUID>

Mode

FQDN Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

FQDN Address Object

Description

Clear address object UUID.

Example

no uuid

Syntax

name <ADDR_FQDN_NAME>

Mode

FQDN Address Object

Description

Set address object name.

Options

<ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*

Example

name "Corp E-mail Server"

Syntax

domain <ADDR_FQDN>

Mode

FQDN Address Object

Description

Set address object fully qualified domain name (FQDN).

Options

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

Example

domain www.sonicwall.com

Syntax

no domain

Mode

FQDN Address Object

Description

Clear address object fully qualified domain name (FQDN).

Example

no domain

Syntax

zone <ZONE_NAME>

Mode

FQDN Address Object

Description

Set address object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

zone WAN

Syntax

dns-ttl <UINT16>

Mode

FQDN Address Object

Description

Manually set DNS entries' TTL.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

dns-ttl 120

Syntax

no dns-ttl

Mode

FQDN Address Object

Description

Disable manually set DNS entries' TTL.

Example

no dns-ttl

Syntax

uuid <UUID>

Mode

IPV6 Address Object

Description

Set address object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

IPV6 Address Object

Description

Clear address object UUID.

Example

no uuid

Syntax

name <ADDR_HOST_NETWORK_RANGE_NAME>

Mode

IPV6 Address Object

Description

Set address object name.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

Example

name "Corp E-mail Server"

Syntax

host <ADDR_HOST>

Mode

IPV6 Address Object

Description

Set address object host IP.

Options

<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

host fe80::217:c5ff:fec2

Syntax

no host

Mode

IPV6 Address Object

Description

Clear address object host IP.

Example

no host

Syntax

range <ADDR_BEGIN> <ADDR_END>

Mode

IPv6 Address Object

Description

Set address object range.

Options

- <ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*
- <ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n*

Example

range fe80::217:c5ff:fecl fe80::217:c5ff:ffff

Syntax

no range

Mode

IPv6 Address Object

Description

Clear address object range.

Example

no range

Syntax

network <ADDR_NETWORK> <ADDR_PREFIX_LEN>

Mode

IPv6 Address Object

Description

Set address object network.

Options

- <ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
- <ADDR_PREFIX_LEN> Network prefix length in decimal or CIDR form: D OR /D.
Max: 128
Example: *128*

Example

```
network fe80::217:c5ff:fec1 /64
```

Syntax

```
no network
```

Mode

IPV6 Address Object

Description

Clear address object network.

Example

```
no network
```

Syntax

```
zone <ZONE_NAME>
```

Mode

IPV6 Address Object

Description

Set address object zone.

Options

```
<ZONE_NAME> Zone object name.  
Example: DMZ
```

Example

```
zone WAN
```

Syntax

```
uuid <UUID>
```

Mode

IPV4 Address Group

Description

Set address group UUID.

Options

```
<UUID> Universally Unique Identifier (UUID).  
Min: 36  
Max: 36  
Example: 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

no uuid

Mode

IPV4 Address Group

Description

Clear address group UUID.

Example

no uuid

Syntax

name <ADDR_GROUP_NAME>

Mode

IPV4 Address Group

Description

Set address group name.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

name "Corporate Servers "

Syntax

no address-object ipv4 <ADDR_HOST_NETWORK_RANGE_NAME> [href <WORD>]

Mode

IPV4 Address Group
IPV6 Address Group

Description

Remove an IPv4 address object from group.

Options

<ADDR_HOST_NETWORK_RANGE_NAME> Host/network/range address object name.
Example: *Web Server*

href Address object ipv4 href.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no address-object ipv4 "Corp E-mail Server"

Syntax

address-object ipv4 <ADDR_HOST_NETWORK_RANGE_NAME> [href <WORD>]

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an IPv4 address object to group.

Options

<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
href	Address object ipv4 href.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
address-object ipv4 "Corp E-mail Server"
```

Syntax

```
no address-object mac <ADDR_MAC_NAME> [ href <WORD> ]
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Remove a MAC address object from group.

Options

<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>
href	Address object mac href.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
no address-object mac "Corp E-mail Server"
```

Syntax

```
address-object mac <ADDR_MAC_NAME> [ href <WORD> ]
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Assign an MAC address object to group.

Options

<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>
href	Address object mac href.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
address-object mac "Corp E-mail Server"
```

Syntax

```
no address-object fqdn <ADDR_FQDN_NAME> [ href <WORD> ]
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Remove a FQDN address object from group.

Options

- <ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*
- href Address object fqdn href.
- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no address-object fqdn "Corp E-mail Server"

Syntax

address-object fqdn <ADDR_FQDN_NAME> [href <WORD>]

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an FQDN address object to group.

Options

- <ADDR_FQDN_NAME> FQDN address object name.
Example: *www.example.com*
- href Address object fqdn href.
- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

address-object fqdn "Corp E-mail Server"

Syntax

no address-group ipv4 <ADDR_GROUP_NAME> [href <WORD>]

Mode

IPV4 Address Group
IPV6 Address Group

Description

Remove an IPv4 address group from group.

Options

- <ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*
- href Address group ipv4 href.
- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no address-group ipv4 "Corp Web Servers"

Syntax

```
address-group ipv4 <ADDR_GROUP_NAME> [ href <WORD> ]
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Assign an IPv4 address group to group.

Options

<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
href	Address group ipv4 href.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
address-group ipv4 "Corp Web Servers"
```

Syntax

```
no address-group-members
```

Mode

IPV4 Address Group
IPV6 Address Group

Description

Remove all IPv4 address group from group.

Example

```
no address-group-members
```

Syntax

```
uuid <UUID>
```

Mode

IPV6 Address Group

Description

Set address group UUID.

Options

<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

IPV6 Address Group

Description

Clear address group UUID.

Example

```
no uuid
```

Syntax

```
name <ADDR_GROUP_NAME>
```

Mode

IPV6 Address Group

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

```
name "Corporate Servers "
```

Syntax

```
no address-object ipv6 <ADDR_NAME> [ href <WORD> ]
```

Mode

IPV4 Address Group

IPV6 Address Group

Description

Remove an IPv6 address object from group.

Options

<ADDR_NAME> Address object name.
Example: *Web Server*

href Address object ipv6 href.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no address-object ipv6 "Corp E-mail Server"
```

Syntax

```
address-object ipv6 <ADDR_NAME> [ href <WORD> ]
```

Mode

IPV4 Address Group

IPV6 Address Group

Description

Assign an IPv6 address object to group.

Options

<ADDR_NAME> Address object name.
Example: *Web Server*

href Address object ipv6 href.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
address-object ipv6 "Corp E-mail Server"
```

Syntax

```
no address-group ipv6 <ADDR_GROUP_NAME> [ href <WORD> ]
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Remove an IPv6 address group from group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

href Address group ipv6 href.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no address-group ipv6 "Corp Web Servers"
```

Syntax

```
address-group ipv6 <ADDR_GROUP_NAME> [ href <WORD> ]
```

Mode

IPv4 Address Group
IPv6 Address Group

Description

Assign an IPv6 address group to group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

href Address group ipv6 href.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
address-group ipv6 "Corp Web Servers"
```

Syntax

```
scheduler
```

Mode

Config

Description

Enter Scheduler Mode.

Example

scheduler

Syntax

schedule [uuid] <SCHED_NAME>

Mode

Scheduler
Config

Description

Add/Edit a Schedule.

Options

- uuid* Edit a schedule object by UUID.
- <SCHED_NAME>* Schedule object name.
Example: *Work Hours*

Example

schedule "Contract Schedule"

Syntax

no schedule [uuid] <SCHED_NAME>

Mode

Scheduler
Config

Description

Delete a schedule.

Options

- uuid* Delete a schedule object by UUID.
- <SCHED_NAME>* Schedule object name.
Example: *Work Hours*

Example

no schedule "Maintenance Schedule"

Syntax

no schedules

Mode

Scheduler
Config

Description

Delete all custom schedules.

Example

no schedules

Syntax

name <*SCHED_NAME*>

Mode

Schedule

Description

Schedule object name.

Options

<*SCHED_NAME*> Schedule object name.
Example: *Work Hours*

Example

name "Contract Schedule"

Syntax

uuid <*UUID*>

Mode

Schedule

Description

Set schedule object UUID.

Options

<*UUID*> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0b00-c0eae49ce84c

Syntax

no uuid

Mode

Schedule

Description

Clear schedule object UUID.

Example

no uuid

Syntax

occurs { mixed | once | recurring }

Mode

Schedule

Description

Set schedule occurrence.

Options

- mixed*** Set for both recurring schedule and single occurrence.
- once*** Set for single occurrence.
- recurring*** Set for recurring schedule.

Example

occurs recurring

Syntax

event <TIME_YYYYMMDDHHMM> <TIME_YYYYMMDDHHMM>

Mode

- One Time Schedule
- Mixed Schedule

Description

Enter the start and end date and time of a one time event.

Options

- <TIME_YYYYMMDDHHMM>** Timestamp in the form: YYYY:MM:DD:HH:MM.
Example: *2010:06:30:23:30*
- <TIME_YYYYMMDDHHMM>** Timestamp in the form: YYYY:MM:DD:HH:MM.
Example: *2010:06:30:23:30*

Example

event 2010:06:01:00:00 2010:06:02:00:00

Syntax

recurring <TIME_HHMM> <TIME_HHMM> { { [sun] [mon] [tue] [wed] [thu] [fri] [sat] } | all }

Mode

- Mixed Schedule
- Recurring Schedule

Description

Add to the list of applicable days and start and stop time of the schedule.

Options

- <TIME_HHMM>** Time in the form: DD:DD.
Example: *12:00*
- <TIME_HHMM>** Time in the form: DD:DD.
Example: *12:00*

- sun*** Day of the week.
- mon*** Day of the week.
- tue*** Day of the week.
- wed*** Day of the week.
- thu*** Day of the week.
- fri*** Day of the week.
- sat*** Day of the week.

- all*** Everyday.

Example

recurring 12:00 18:00 mon tue wed thu fri

Syntax

no recurring <TIME_HHMM> <TIME_HHMM> { { [sun] [mon] [tue] [wed] [thu] [fri] [sat] } | all }

Mode

Mixed Schedule
Recurring Schedule

Description

Remove from the schedule an entry by specifying applicable days and start and stop time.

Options

<TIME_HHMM> Time in the form: DD:DD.
Example: *12:00*

<TIME_HHMM> Time in the form: DD:DD.
Example: *12:00*

sun Day of the week.
mon Day of the week.
tue Day of the week.
wed Day of the week.
thu Day of the week.
fri Day of the week.
sat Day of the week.

all Everyday.

Example

no recurring 12:00 18:00 mon tue wed thu fri

Syntax

no recurrings

Mode

Mixed Schedule
Recurring Schedule

Description

Remove all recurring from the schedule.

Example

no recurrings

Syntax

no service-object [uuid] <SVC_NAME>

Mode

Config

Description

Delete a service object.

Options

uuid Delete a sevice object by UUID.

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

```
no service-object "Corp E-mail Server"
```

Syntax

```
no service-objects
```

Mode

Config

Description

Delete all custom service objects.

Example

```
no service-objects
```

Syntax

```
service-object [ uuid ] <SVC_NAME> [ 6over4 | ah | custom <UINT8> | eigrp | esp | gre | icmp { { { address-mask-reply | address-mask-request | alternative-host | datagram-error | destination-unreachable | domain-name | domain-name-reply | echo-reply | echo-request | info-reply | info-request | mobile-host-redirect | mobile-registration-reply | mobile-registration-request | none | parameter-problem | redirect | router-advertise | router-solicit | source-quench | time-exceeded | timestamp | timestamp-reply | traceroute } } } | icmpv6 { { { certification-path-advertisement | certification-path-solicitation | destination-unreachable | echo-reply | echo-request | fmipv6 | home-discover-reply | home-discover-request | inverse-nd-advertisement | inverse-nd-solicitation | mobile-prefix-advertisement | mobile-prefix-solicitation | multicast-listener-done | multicast-listener-query | multicast-listener-report | multicast-router-advertisement | multicast-router-solicitation | multicast-router-termination | neighbour-advertisement | neighbour-solicitation | node-query | node-response | packet-too-big | parameter-problem | redirect | router-advertisement | router-renumbering | router-solicitation | rpl-control | time-exceeded | v2-multicast-listener-report } } } | icmpv6-custom <UINT16> | igmp { { { leave-group | member-query | none | v1-member-report | v2-member-report | v3-member-report } } } | ipcomp | l2tp | ospf { { { database-description | hello | link-state-acknowledge | link-state-request | link-state-update | none } } } | pim { { { assert | bootstrap | candidate-rp | graft | graft-acknowledge | hello | join-prune | none | register | register-stop | state-refresh } } } | tcp <SVC_PORT_BEGIN> <SVC_PORT_END> | udp <SVC_PORT_BEGIN> <SVC_PORT_END> ]
```

Mode

Config

Description

Add/edit firewall and service object and enter configuration mode.

Options

uuid	Edit a service object by UUID.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
6over4	Service object 6over4.
ah	Service object AH.
custom	Custom service object.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
eigrp	Service object EIGRP.
esp	Service object ESP.
gre	Service object GRE.
icmp	Service object ICMP.
address-mask-reply	ICMP with sub-type of address mask reply.

<i>address-mask-request</i>	ICMP with sub-type of address mask request.
<i>alternative-host</i>	ICMP with sub-type of alternative address for host.
<i>datagram-error</i>	ICMP with sub-type of datagram error.
<i>destination-unreachable</i>	ICMP with sub-type of destination unreachable.
<i>domain-name</i>	ICMP with sub-type of domain name.
<i>domain-name-reply</i>	ICMP with sub-type of domain name reply.
<i>echo-reply</i>	ICMP with sub-type of echo reply.
<i>echo-request</i>	ICMP with sub-type of echo request.
<i>info-reply</i>	ICMP with sub-type of info reply.
<i>info-request</i>	ICMP with sub-type of info request.
<i>mobile-host-redirect</i>	ICMP with sub-type of mobile host redirect.
<i>mobile-registration-reply</i>	ICMP with sub-type of mobile registration reply.
<i>mobile-registration-request</i>	ICMP with sub-type of mobile registration request.
<i>none</i>	ICMP with sub-type of none.
<i>parameter-problem</i>	ICMP with sub-type of parameter problem.
<i>redirect</i>	ICMP with sub-type of redirect.
<i>router-advertise</i>	ICMP with sub-type of router advertise.
<i>router-solicit</i>	ICMP with sub-type of router solicit.
<i>source-quench</i>	ICMP with sub-type of source quench.
<i>time-exceeded</i>	ICMP with sub-type of time exceeded.
<i>timestamp</i>	ICMP with sub-type of timestamp.
<i>timestamp-reply</i>	ICMP with sub-type of timestamp reply.
<i>traceroute</i>	ICMP with sub-type of traceroute.
<i>icmpv6</i>	Service object ICMPV6/ND.
<i>certification-path-advertisement</i>	ICMPV6 with sub-type of certification path advertisement message.
<i>certification-path-solicitation</i>	ICMPV6 with sub-type of certification path solicitation message.
<i>destination-unreachable</i>	ICMPV6 with sub-type of destination unreachable.
<i>echo-reply</i>	ICMPV6 with sub-type of echo reply.
<i>echo-request</i>	ICMPV6 with sub-type of echo request.
<i>fmipv6</i>	ICMPV6 with sub-type of FMIPv6 messages.
<i>home-discover-reply</i>	ICMPV6 with sub-type of home agent address discovery reply message.
<i>home-discover-request</i>	ICMPV6 with sub-type of home agent address discovery request message.
<i>inverse-nd-advertisement</i>	ICMPV6 with sub-type of inverse ND advertisement message.

<i>inverse-nd-solicitation</i>	ICMPV6 with sub-type of inverse ND solicitation message.
<i>mobile-prefix-advertisement</i>	ICMPV6 with sub-type of mobile prefix advertisement.
<i>mobile-prefix-solicitation</i>	ICMPV6 with sub-type of mobile prefix solicitation.
<i>multicast-listener-done</i>	ICMPV6 with sub-type of multicast listener done.
<i>multicast-listener-query</i>	ICMPV6 with sub-type of multicast listener query.
<i>multicast-listener-report</i>	ICMPV6 with sub-type of multicast listener report.
<i>multicast-router-advertisement</i>	ICMPV6 with sub-type of multicast router advertisement.
<i>multicast-router-solicitation</i>	ICMPV6 with sub-type of multicast router solicitation.
<i>multicast-router-termination</i>	ICMPV6 with sub-type of multicast router termination.
<i>neighbour-advertisement</i>	ICMPV6 with sub-type of neighbour advertisement.
<i>neighbour-solicitation</i>	ND with sub-type of neighbour solicitation.
<i>node-query</i>	ICMPV6 with sub-type of ICMP node information query.
<i>node-response</i>	ICMPV6 with sub-type of ICMP node information response.
<i>packet-too-big</i>	ICMPV6 with sub-type of packet too big.
<i>parameter-problem</i>	ICMPV6 with sub-type of parameter problem.
<i>redirect</i>	ND with sub-type of redirect.
<i>router-advertisement</i>	ND with sub-type of router advertisement.
<i>router-renumbering</i>	ICMPV6 with sub-type of router renumbering.
<i>router-solicitation</i>	ND with sub-type of router solicitation.
<i>rpl-control</i>	ICMPV6 with sub-type of RPL control message.
<i>time-exceeded</i>	ICMPV6 with sub-type of time exceeded.
<i>v2-multicast-listener-report</i>	ICMPV6 with sub-type of version 2 multicast listener report.
<i>icmpv6-custom</i> <i><UINT16></i>	Service object ICMPV6/ND with custom sub-type. Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>igmp</i>	Service object IGMP.
<i>leave-group</i>	IGMP with sub-type of leave group.
<i>member-query</i>	IGMP with sub-type of member query.
<i>none</i>	IGMP with sub-type of none.
<i>v1-member-report</i>	IGMP with sub-type of v1 member report.
<i>v2-member-report</i>	IGMP with sub-type of v2 member report.
<i>v3-member-report</i>	IGMP with sub-type of v3 member report.
<i>ipcomp</i>	Service object IPCOMP.
<i>l2tp</i>	Service object l2tp.
<i>ospf</i>	Service object OSPF.

database-description	OSPF with sub-type of database description.
hello	OSPF with sub-type of hello.
link-state-acknowledge	OSPF with sub-type of link state acknowledge.
link-state-request	OSPF with sub-type of link state request.
link-state-update	OSPF with sub-type of link state update.
none	OSPF with sub-type of none.
pim	Service object PIM.
assert	PIM with sub-type of assert.
bootstrap	PIM with sub-type of bootstrap.
candidate-rp	PIM with sub-type of candidate rp.
graft	PIM with sub-type of graft.
graft-acknowledge	PIM with sub-type of graft acknowledge.
hello	PIM with sub-type of hello.
join-prune	PIM with sub-type of join/prune.
none	PIM with sub-type of none.
register	PIM with sub-type of register.
register-stop	PIM with sub-type of register stop.
state-refresh	PIM with sub-type of state refresh.
tcp	Service object TCP.
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: 80
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: 80
udp	Service object UDP.
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: 80
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: 80

Example

```
service-object "Web Server" TCP 80 80
```

Syntax

```
no service-group [ uuid ] <SVC_GROUP_NAME>
```

Mode

Config

Description

Delete a service group.

Options

uuid Delete a service group by UUID.

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
no service-group "Corporate Servers"
```

Syntax

```
no service-groups
```

Mode

Config

Description

Delete all custom service groups.

Example

```
no service-groups
```

Syntax

```
service-group [ uuid ] <SVC_GROUP_NAME>
```

Mode

Config

Description

Add/edit service group and enter configuration mode.

Options

uuid Edit a service group by UUID.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
service-group "Corporate Servers"
```

Syntax

```
name <SVC_NAME>
```

Mode

Service Object

Description

Set service object name.

Options

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

```
name "Corp E-mail Server "
```

Syntax

uuid <UUID>

Mode

Service Object

Description

Set service object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Service Object

Description

Clear service object UUID.

Example

no uuid

Syntax

custom <UINT8>

Mode

Service Object

Description

Set service object as custom and specify.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

custom 123

Syntax

icmp { { { address-mask-reply | address-mask-request | alternative-host | datagram-error | destination-unreachable | domain-name | domain-name-reply | echo-reply | echo-request | info-reply | info-request | mobile-host-redirect | mobile-registration-reply | mobile-registration-request | none | parameter-problem | redirect | router-advertise | router-solicit | source-quench | time-exceeded | timestamp | timestamp-reply | traceroute } } }

Mode

Service Object

Description

Set service object as ICMP and specify sub type.

Options

<i>address-mask-reply</i>	ICMP with sub-type of address mask reply.
<i>address-mask-request</i>	ICMP with sub-type of address mask request.
<i>alternative-host</i>	ICMP with sub-type of alternative address for host.
<i>datagram-error</i>	ICMP with sub-type of datagram error.
<i>destination-unreachable</i>	ICMP with sub-type of destination unreachable.
<i>domain-name</i>	ICMP with sub-type of domain name.
<i>domain-name-reply</i>	ICMP with sub-type of domain name reply.
<i>echo-reply</i>	ICMP with sub-type of echo reply.
<i>echo-request</i>	ICMP with sub-type of echo request.
<i>info-reply</i>	ICMP with sub-type of info reply.
<i>info-request</i>	ICMP with sub-type of info request.
<i>mobile-host-redirect</i>	ICMP with sub-type of mobile host redirect.
<i>mobile-registration-reply</i>	ICMP with sub-type of mobile registration reply.
<i>mobile-registration-request</i>	ICMP with sub-type of mobile registration request.
<i>none</i>	ICMP with sub-type of none.
<i>parameter-problem</i>	ICMP with sub-type of parameter problem.
<i>redirect</i>	ICMP with sub-type of redirect.
<i>router-advertise</i>	ICMP with sub-type of router advertise.
<i>router-solicit</i>	ICMP with sub-type of router solicit.
<i>source-quench</i>	ICMP with sub-type of source quench.
<i>time-exceeded</i>	ICMP with sub-type of time exceeded.
<i>timestamp</i>	ICMP with sub-type of timestamp.
<i>timestamp-reply</i>	ICMP with sub-type of timestamp reply.
<i>traceroute</i>	ICMP with sub-type of traceroute.

Example

```
icmp echo-reply
```

Syntax

```
igmp { { { leave-group | member-query | none | v1-member-report | v2-member-report | v3-member-report } } }
```

Mode

Service Object

Description

Set service object as IGMP and specify sub type.

Options

<i>leave-group</i>	IGMP with sub-type of leave group.
<i>member-query</i>	IGMP with sub-type of member query.
<i>none</i>	IGMP with sub-type of none.
<i>v1-member-report</i>	IGMP with sub-type of v1 member report.
<i>v2-member-report</i>	IGMP with sub-type of v2 member report.
<i>v3-member-report</i>	IGMP with sub-type of v3 member report.

Example

igmp member-query

Syntax

tcp <SVC_PORT_BEGIN> <SVC_PORT_END>

Mode

Service Object

Description

Set service object as TCP.

Options

<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

tcp 1 80

Syntax

udp <SVC_PORT_BEGIN> <SVC_PORT_END>

Mode

Service Object

Description

Set service object as UDP.

Options

<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

udp 1 80

Syntax

6over4

Mode

Service Object

Description

Set service object as 6over4.

Example

6over4

Syntax

gre

Mode

Service Object

Description

Set service object as GRE.

Example

gre

Syntax

esp

Mode

Service Object

Description

Set service object as ESP.

Example

esp

Syntax

ah

Mode

Service Object

Description

Set service object as AH.

Example

ah

Syntax

```
icmpv6 { { { certification-path-advertisement | certification-path-solicitation | destination-unreachable | echo-reply | echo-request | fmipv6 | home-discover-reply | home-discover-request | inverse-nd-advertisement | inverse-nd-solicitation | mobile-prefix-advertisement | mobile-prefix-solicitation | multicast-listener-done | multicast-listener-query | multicast-listener-report | multicast-router-advertisement | multicast-router-solicitation | multicast-router-termination | neighbour-advertisement | neighbour-solicitation | node-query | node-response | packet-too-big | parameter-problem | redirect | router-advertisement | router-renumbering | router-solicitation | rpl-control | time-exceeded | v2-multicast-listener-report } } }
```

Mode

Service Object

Description

Set service object as ICMPV6.

Options

<i>certification-path-advertisement</i>	ICMPV6 with sub-type of certification path advertisement message.
<i>certification-path-solicitation</i>	ICMPV6 with sub-type of certification path solicitation message.
<i>destination-unreachable</i>	ICMPV6 with sub-type of destination unreachable.
<i>echo-reply</i>	ICMPV6 with sub-type of echo reply.
<i>echo-request</i>	ICMPV6 with sub-type of echo request.
<i>fmipv6</i>	ICMPV6 with sub-type of FMIPv6 messages.
<i>home-discover-reply</i>	ICMPV6 with sub-type of home agent address discovery reply message.
<i>home-discover-request</i>	ICMPV6 with sub-type of home agent address discovery request message.
<i>inverse-nd-advertisement</i>	ICMPV6 with sub-type of inverse ND advertisement message.
<i>inverse-nd-solicitation</i>	ICMPV6 with sub-type of inverse ND solicitation message.
<i>mobile-prefix-advertisement</i>	ICMPV6 with sub-type of mobile prefix advertisement.
<i>mobile-prefix-solicitation</i>	ICMPV6 with sub-type of mobile prefix solicitation.
<i>multicast-listener-done</i>	ICMPV6 with sub-type of multicast listener done.
<i>multicast-listener-query</i>	ICMPV6 with sub-type of multicast listener query.
<i>multicast-listener-report</i>	ICMPV6 with sub-type of multicast listener report.
<i>multicast-router-advertisement</i>	ICMPV6 with sub-type of multicast router advertisement.
<i>multicast-router-solicitation</i>	ICMPV6 with sub-type of multicast router solicitation.
<i>multicast-router-termination</i>	ICMPV6 with sub-type of multicast router termination.
<i>neighbour-advertisement</i>	ICMPV6 with sub-type of neighbour advertisement.
<i>neighbour-solicitation</i>	ND with sub-type of neighbour solicitation.
<i>node-query</i>	ICMPV6 with sub-type of ICMP node information query.
<i>node-response</i>	ICMPV6 with sub-type of ICMP node information response.
<i>packet-too-big</i>	ICMPV6 with sub-type of packet too big.
<i>parameter-problem</i>	ICMPV6 with sub-type of parameter problem.
<i>redirect</i>	ND with sub-type of redirect.
<i>router-advertisement</i>	ND with sub-type of router advertisement.

<i>router-renumbering</i>	ICMPV6 with sub-type of router renumbering.
<i>router-solicitation</i>	ND with sub-type of router solicitation.
<i>rpl-control</i>	ICMPV6 with sub-type of RPL control message.
<i>time-exceeded</i>	ICMPV6 with sub-type of time exceeded.
<i>v2-multicast-listener-report</i>	ICMPV6 with sub-type of version 2 multicast listener report.

Example

```
icmpv6 echo-reply
```

Syntax

```
icmpv6-custom <UINT16>
```

Mode

Service Object

Description

Set service object as ICMPV6.

Options

```
<UINT16> Integer in the form: D OR 0xHHHH.  
Example: 123
```

Example

```
icmpv6-custom 6
```

Syntax

```
eigrp
```

Mode

Service Object

Description

Set service object as EIGRP.

Example

```
eigrp
```

Syntax

```
ospf { { { database-description | hello | link-state-acknowledge | link-state-request | link-state-update | none } } }
```

Mode

Service Object

Description

Set service object as OSPF and specify sub type.

Options

```
database-description OSPF with sub-type of database description.
```

<i>hello</i>	OSPF with sub-type of hello.
<i>link-state-acknowledge</i>	OSPF with sub-type of link state acknowledge.
<i>link-state-request</i>	OSPF with sub-type of link state request.
<i>link-state-update</i>	OSPF with sub-type of link state update.
<i>none</i>	OSPF with sub-type of none.

Example

```
ospf hello
```

Syntax

```
pim { { { assert | bootstrap | candidate-rp | graft | graft-acknowledge | hello | join-prune | none | register | register-stop | state-refresh } } }
```

Mode

Service Object

Description

Set service object as PIM and specify sub type.

Options

<i>assert</i>	PIM with sub-type of assert.
<i>bootstrap</i>	PIM with sub-type of bootstrap.
<i>candidate-rp</i>	PIM with sub-type of candidate rp.
<i>graft</i>	PIM with sub-type of graft.
<i>graft-acknowledge</i>	PIM with sub-type of graft acknowledge.
<i>hello</i>	PIM with sub-type of hello.
<i>join-prune</i>	PIM with sub-type of join/prune.
<i>none</i>	PIM with sub-type of none.
<i>register</i>	PIM with sub-type of register.
<i>register-stop</i>	PIM with sub-type of register stop.
<i>state-refresh</i>	PIM with sub-type of state refresh.

Example

```
pim none
```

Syntax

```
l2tp
```

Mode

Service Object

Description

Set service object as l2tp.

Example

l2tp

Syntax

ipcomp

Mode

Service Object

Description

Set service object as ipcomp.

Example

ipcomp

Syntax

name <*SVC_GROUP_NAME*>

Mode

Service Group

Description

Set service group name.

Options

<*SVC_GROUP_NAME*> Service object group name.
Example: *VOIP*

Example

name "Corporate Servers "

Syntax

uuid <*UUID*>

Mode

Service Group

Description

Set service group UUID.

Options

<*UUID*> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid *f40b27d6-b8b9-a4fc-0300-c0eae49ce84c*

Syntax

no uuid

Mode

Service Group

Description

Clear service group UUID.

Example

no uuid

Syntax

no service-object <SVC_NAME>

Mode

Service Group

Description

Remove service object from group.

Options

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

no service-object "Corp E-mail Server"

Syntax

service-object <SVC_NAME>

Mode

Service Group

Description

Assign service object to group.

Options

<SVC_NAME> Service object name.
Example: *HTTPS*

Example

service-object "Corp E-mail Server"

Syntax

no service-group <SVC_GROUP_NAME>

Mode

Service Group

Description

Remove service group from group.

Options

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
no service-group "Corp Web Servers"
```

Syntax

```
service-group <SVC_GROUP_NAME>
```

Mode

Service Group

Description

Assign service group to group.

Options

<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

Example

```
service-group "Corp Web Servers"
```

Syntax

```
no service-objects
```

Mode

Service Group

Description

Remove all service objects from group.

Example

```
no service-objects
```

Syntax

```
no service-groups
```

Mode

Service Group

Description

Remove all service groups from group.

Example

```
no service-groups
```

Syntax

```
zone [ uuid ] <ZONE_NAME>
```

Mode

Config

Description

Add/Edit a Zone.

Options

- `uuid` Edit a zone by UUID.
- `<ZONE_NAME>` Zone object name.
Example: *DMZ*

Example

`zone "Office Servers"`

Syntax

`no zone [ uuid ] <ZONE_NAME>`

Mode

Config

Description

Delete a custom zone.

Options

- `uuid` Delete a custom zone by UUID.
- `<ZONE_NAME>` Zone object name.
Example: *DMZ*

Example

`no zone "Office Servers"`

Syntax

`no zones`

Mode

Config

Description

Delete all custom zones.

Example

`no zones`

Syntax

`guest-services`

Mode

Zone

Description

Enter configuration mode.

Example

`guest-services`

Syntax

wireless

Mode

Zone

Description

Enter wireless zone configuration mode.

Example

wireless

Syntax

uuid <UUID>

Mode

Zone

Description

Set zone object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Zone

Description

Clear zone object UUID.

Example

no uuid

Syntax

name <ZONE_NAME>

Mode

Zone

Description

Set Zone Name.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
name guest
```

Syntax

```
security-type { encrypted | public | sslvpn | trusted | untrusted | wireless }
```

Mode

Zone

Description

Set zone security type.

Options

encrypted VPN zone.

public Public zone.

sslvpn SSLVPN zone.

trusted Trusted zone.

untrusted WAN/MULTICAST zone.

wireless Wireless zone.

Example

```
security-type public
```

Syntax

```
no security-type
```

Mode

Zone

Description

Disable zone security type.

Example

```
no security-type
```

Syntax

```
interface-trust
```

Mode

Zone

Description

Enable allow interface trust.

Example

```
interface-trust
```

Syntax

```
no interface-trust
```

Mode

Zone

Description

Disable allow interface trust.

Example

```
no interface-trust
```

Syntax

```
auto-generate-access-rules { allow-from-higher | allow-from-to-equal | allow-to-lower | deny-from-lower }
```

Mode

Zone

Description

Enable auto generate access rules.

Options

<i>allow-from-higher</i>	Allow traffic from zones with higher trust level.
<i>allow-from-to-equal</i>	Allow traffic between zones with the same trust level.
<i>allow-to-lower</i>	Allow traffic to zones with lower trust level.
<i>deny-from-lower</i>	Deny traffic from zones with lower trust level.

Example

```
auto-generate-access-rules allow-from-to-equal
```

Syntax

```
no auto-generate-access-rules { allow-from-higher | allow-from-to-equal | allow-to-lower | deny-from-lower }
```

Mode

Zone

Description

Disable auto generate access rules.

Options

<i>allow-from-higher</i>	Allow traffic from zones with higher trust level.
<i>allow-from-to-equal</i>	Allow traffic between zones with the same trust level.
<i>allow-to-lower</i>	Allow traffic to zones with lower trust level.

deny-from-lower Deny traffic from zones with lower trust level.

Example

```
no auto-generate-access-rules allow-from-to-equal
```

Syntax

```
websense-content-filtering
```

Mode

Zone

Description

Enable enforce websense enterprise content filtering service.

Example

```
websense-content-filtering
```

Syntax

```
no websense-content-filtering
```

Mode

Zone

Description

Disable enforce websense enterprise content filtering service.

Example

```
no websense-content-filtering
```

Syntax

```
gateway-anti-virus
```

Mode

Zone

Description

Enable gateway anti-virus service.

Example

```
gateway-anti-virus
```

Syntax

```
no gateway-anti-virus
```

Mode

Zone

Description

Disable gateway anti-virus service.

Example

```
no gateway-anti-virus
```

Syntax

```
intrusion-prevention
```

Mode

Zone

Description

Enable intrusion prevention service.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

Zone

Description

Disable intrusion prevention service.

Example

```
no intrusion-prevention
```

Syntax

```
app-control
```

Mode

Zone

Description

Enable app control service.

Example

```
app-control
```

Syntax

```
no app-control
```

Mode

Zone

Description

Disable app control service.

Example

```
no app-control
```

Syntax

anti-spyware

Mode

Zone

Description

Enable Anti-Spyware Service.

Example

anti-spyware

Syntax

no anti-spyware

Mode

Zone

Description

Disable anti-spyware service.

Example

no anti-spyware

Syntax

create-group-vpn

Mode

Zone

Description

Enable automatic creation of group VPN for this zone.

Example

create-group-vpn

Syntax

no create-group-vpn

Mode

Zone

Description

Disable automatic creation of group VPN for this zone.

Example

no create-group-vpn

Syntax

ssl-control

Mode

Zone

Description

Enable SSL-Control on this zone.

Example

ssl-control

Syntax

no ssl-control

Mode

Zone

Description

Disable SSL-Control on this zone.

Example

no ssl-control

Syntax

dpi-ssl-client

Mode

Zone

Description

Enable SSL client inspection.

Example

dpi-ssl-client

Syntax

no dpi-ssl-client

Mode

Zone

Description

Disable SSL client inspection.

Example

no dpi-ssl-client

Syntax

dpi-ssl-server

Mode

Zone

Description

Enable SSL server inspection.

Example

```
dpi-ssl-server
```

Syntax

```
no dpi-ssl-server
```

Mode

Zone

Description

Disable SSL server inspection.

Example

```
no dpi-ssl-server
```

Syntax

```
sslvpn-access
```

Mode

Zone

Description

Enable SSL-VPN access for this zone.

Example

```
sslvpn-access
```

Syntax

```
no sslvpn-access
```

Mode

Zone

Description

Disable SSL-VPN access for this zone.

Example

```
no sslvpn-access
```

Syntax

```
enable
```

Mode

Guest Services

Description

Enable guest services.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Guest Services

Description

Disable guest services.

Example

```
no enable
```

Syntax

```
inter-guest
```

Mode

Guest Services

Description

Enable inter-guest communication.

Example

```
inter-guest
```

Syntax

```
no inter-guest
```

Mode

Guest Services

Description

Disable inter-guest communication.

Example

```
no inter-guest
```

Syntax

```
external-auth
```

Mode

Guest Services

Description

Enter its configuration mode.

Example

external-auth

Syntax

captive-portal-authentication

Mode

Guest Services

Description

Enter its configuration mode.

Example

captive-portal-authentication

Syntax

policy-page-non-authentication

Mode

Guest Services

Description

Enter its configuration mode.

Example

policy-page-non-authentication

Syntax

enable

Mode

External Guest Authentication

Description

Enable external auth zone mode.

Example

enable

Syntax

no enable

Mode

External Guest Authentication

Description

Disable external auth zone mode.

Example

no enable

Syntax

```
client-redirect { http | https }
```

Mode

External Guest Authentication

Description

Set local web server settings for client redirect.

Options

http Set protocol HTTP.

https Set protocol HTTPS.

Example

```
client-redirect https
```

Syntax

```
web-server-1 protocol { http | https } { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_FQDNHOST_ADDR> | name  
<ADDR_FQDNHOST_ADDR_MIXED> } } [ port <IPV4_PORT> ]
```

Mode

External Guest Authentication

Description

Set the external web server 1 protocol.

Options

http	Set protocol HTTP.
https	Set protocol HTTPS.
ipv6	IPv6 address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
host <ADDR_FQDNHOST_ADDR>	Configure the external web server IP addresses or hostname. FQDN/host address object name. Example: <i>Web Server</i>
name <ADDR_FQDNHOST_ADDR_MIXED>	Configure webserver to named address object. FQDN/host address object name. Example: <i>Web Server</i>
port <IPV4_PORT>	Configure the external web server port. Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
web-server-1 protocol https host 192.168.168.152 port 443
```

Syntax

```
no web-server-1
```

Mode

External Guest Authentication

Description

Disable the external web server 1.

Example

```
no web-server-1
```

Syntax

```
web-server-2 protocol { http | https } { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_FQDNHOST_ADDR> | name <ADDR_FQDNHOST_ADDR_MIXED> } } [ port <IPV4_PORT> ]
```

Mode

External Guest Authentication

Description

Set the external web server 2 protocol.

Options

http	Set protocol HTTP.
https	Set protocol HTTPS.
ipv6	IPv6 address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
host <ADDR_FQDNHOST_ADDR>	Configure the external web server IP addresses or hostname. FQDN/host address object name. Example: <i>Web Server</i>
name <ADDR_FQDNHOST_ADDR_MIXED>	Configure webserver to named address object. FQDN/host address object name. Example: <i>Web Server</i>
port <IPV4_PORT>	Configure the external web server port. Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
web-server-2 protocol https host 192.168.168.152 port 443
```

Syntax

```
no web-server-2
```

Mode

External Guest Authentication

Description

Disable the external web server 2.

Example

```
no web-server-2
```

Syntax

```
web-server timeout <UINT8>
```

Mode

External Guest Authentication

Description

Set the external web server connection timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
web-server timeout 10
```

Syntax

```
message-auth [ enable ] [ method { md5 | sha1 | sha256 } ] [ shared-secret <ENC_PASSWORD> confirm-secret <ENC_PASSWORD> ]
```

Mode

External Guest Authentication

Description

Enable external message authentication.

Options

- enable** Enable external message authentication.
- method** Set external message authentication method.
- md5** Use HMAC - MD5 authentication.
- sha1** Use HMAC - SHA1 authentication.
- sha256** Use HMAC - SHA256 authentication.
- shared-secret** Set external message authentication shared secret.
- <ENC_PASSWORD>** Password.
Example: *secret*
- confirm-secret** Confirm external message authentication shared secret.
- <ENC_PASSWORD>** Password.
Example: *secret*

Example

```
message-auth method md5 shared-secret donttell confirm-secret donttell
```

Syntax

```
no message-auth [ enable ]
```

Mode

External Guest Authentication

Description

Disable external message authentication.

Options

enable Disable external message authentication.

Example

```
no message-auth
```

Syntax

```
social-network [ enable | facebook | google | twitter ]
```

Mode

External Guest Authentication

Description

Enable specified social network login.

Options

enable	Enable social network login.
facebook	Enable Facebook social network login.
google	Enable Google social network login.
twitter	Enable Twitter social network login.

Example

```
social-network
```

Syntax

```
no social-network [ enable | facebook | google | twitter ]
```

Mode

External Guest Authentication

Description

Disable social network login.

Options

enable	Disable social network login.
facebook	Disable Facebook social network login.
google	Disable Google social network login.
twitter	Disable Twitter social network login.

Example

```
no social-network
```

Syntax

```
auth-pages web-server-1 login <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 login page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 login login.html
```

Syntax

```
no auth-pages web-server-1 login
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 login page.

Example

```
no auth-pages web-server-1 login
```

Syntax

```
auth-pages web-server-1 expiration <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 session expiration page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 expiration exp.html
```

Syntax

```
no auth-pages web-server-1 expiration
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 session expiration page.

Example

```
no auth-pages web-server-1 expiration
```

Syntax

```
auth-pages web-server-1 timeout <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 idle timeout page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 timeout idle.html
```

Syntax

```
no auth-pages web-server-1 timeout
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 idle timeout page.

Example

```
no auth-pages web-server-1 timeout
```

Syntax

```
auth-pages web-server-1 max-sessions <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 max sessions page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 max-sessions max.html
```

Syntax

```
no auth-pages web-server-1 max-sessions
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 max sessions page.

Example

```
no auth-pages web-server-1 max-sessions
```

Syntax

```
auth-pages web-server-1 traffic-exceeded <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 1 traffic exceeded page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-1 traffic-exceeded trafficExceeded.html
```

Syntax

```
no auth-pages web-server-1 traffic-exceeded
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 1 traffic exceeded page.

Example

```
no auth-pages web-server-1 traffic-exceeded
```

Syntax

```
auth-pages web-server-2 login <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 login page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 login login.html
```

Syntax

```
no auth-pages web-server-2 login
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 login page.

Example

```
no auth-pages web-server-2 login
```

Syntax

```
auth-pages web-server-2 expiration <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 session expiration page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 expiration exp.html
```

Syntax

```
no auth-pages web-server-2 expiration
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 session expiration page.

Example

```
no auth-pages web-server-2 expiration
```

Syntax

```
auth-pages web-server-2 timeout <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 idle timeout page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 timeout idle.html
```

Syntax

```
no auth-pages web-server-2 timeout
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 idle timeout page.

Example

```
no auth-pages web-server-2 timeout
```

Syntax

```
auth-pages web-server-2 max-sessions <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 max sessions page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 max-sessions max.html
```

Syntax

```
no auth-pages web-server-2 max-sessions
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 max sessions page.

Example

```
no auth-pages web-server-2 max-sessions
```

Syntax

```
auth-pages web-server-2 traffic-exceeded <WORD>
```

Mode

External Guest Authentication

Description

Set the external authentication web server 2 traffic exceeded page.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
auth-pages web-server-2 traffic-exceeded trafficExceeded.html
```

Syntax

```
no auth-pages web-server-2 traffic-exceeded
```

Mode

External Guest Authentication

Description

Disable the external authentication web server 2 traffic exceeded page.

Example

```
no auth-pages web-server-2 traffic-exceeded
```

Syntax

```
web-content redirect { custom <WORD> | use-default }
```

Mode

External Guest Authentication

Description

Configure the Web content redirect message.

Options

custom Set a custom Web content redirect message.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

use-default Use the default Web content redirect message.

Example

```
web-content redirect custom "My custom redirect message"
```

Syntax

```
no web-content redirect use-default
```

Mode

External Guest Authentication

Description

Change the Web content redirect message.

Options

use-default Don't use the default Web content redirect message.

Example

```
no web-content redirect use-default.
```

Syntax

```
web-content server-down { custom <WORD> | use-default }
```

Mode

External Guest Authentication

Description

Configure the Web content redirect message.

Options

- custom** Set a custom Web content server down message.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- use-default** Use the default Web content server down message.

Example

```
web-content server-down custom "My custom server down message"
```

Syntax

```
no web-content server-down use-default
```

Mode

External Guest Authentication

Description

Change the Web content redirect message.

Options

- use-default** Don't use the default Web content server down message.

Example

```
no web-content server-down use-default
```

Syntax

```
logout-expired { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | enable | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable auto-session logout.

Options

- cgi** Set logout CGI.
- web-server-1** Set logout cgi of web server 1.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- web-server-2** Set logout cgi of web server 2.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".

Example: *abc*

<i>enable</i>	Disable Auto-Session Logout.
<i>every</i>	Set auto-logout expired session every (minutes).
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

```
logout-expired every 20
logout-expired cgi web-server-1 expired.cgi
logout-expired cgi web-server-2 expired.cgi
```

Syntax

```
no logout-expired { cgi { web-server-1 | web-server-2 } | enable }
```

Mode

External Guest Authentication

Description

Disable auto-session logout.

Options

<i>cgi</i>	Clear logout CGI.
<i>web-server-1</i>	Clear logout cgi of web server 1.
<i>web-server-2</i>	Clear logout cgi of web server 2.
<i>enable</i>	Disable Auto-Session Logout.

Example

```
no logout-expired
```

Syntax

```
status-check { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | enable | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable server status check.

Options

<i>cgi</i>	Set server status CGI.
<i>web-server-1</i>	Set server status CGI of web server 1.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>web-server-2</i>	Set server status CGI of web server 2.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>enable</i>	Enable server status check.
<i>every</i>	Set check server status every (minutes).

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
status-check every 20
status-check cgi web-server-1 status.cgi
status-check cgi web-server-2 status.cgi
```

Syntax

```
no status-check { cgi { web-server-1 | web-server-2 } | enable }
```

Mode

External Guest Authentication

Description

Disable server status check.

Options

- cgi** Set server status CGI.
- web-server-1** Set server status CGI of web server 1.
- web-server-2** Set server status CGI of web server 2.
- enable** Enable server status check.

Example

```
no status-check
```

Syntax

```
session-sync { cgi { web-server-1 <WORD> | web-server-2 <WORD> } | enable | every <UINT8> }
```

Mode

External Guest Authentication

Description

Enable session synchronization.

Options

- cgi** Set session sync CGI.
- web-server-1** Set session sync CGI of web server 1.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- web-server-2** Set session sync CGI of web server 2.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- enable** Enable session synchronization.
- every** Set synchronize every (minutes).
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*

Example

```
session-sync every 20
session-sync cgi web-server-1 sync.cgi
session-sync cgi web-server-2 sync.cgi
```

Syntax

```
no session-sync { cgi { web-server-1 | web-server-2 } | enable }
```

Mode

External Guest Authentication

Description

Disable session synchronization.

Options

<i>cgi</i>	Set session sync CGI.
<i>web-server-1</i>	Set session sync CGI of web server 1.
<i>web-server-2</i>	Set session sync CGI of web server 2.
<i>enable</i>	Disable session synchronization.

Example

```
no session-sync
```

Syntax

```
enable
```

Mode

Captive Portal Authentication

Description

Enable Captive Portal Authentication.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Captive Portal Authentication

Description

Disable Captive Portal Authentication.

Example

```
no enable
```

Syntax


```
internal-url <WEB_URL>
```

Mode

Captive Portal Authentication

Description

Configure internal captive portal vendor url.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
internal-url http://192.168.168.1/internal.html
```

Syntax

```
no internal-url
```

Mode

Captive Portal Authentication

Description

Clear the internal captive portal vendor url.

Example

```
no internal-url
```

Syntax

```
external-url <WEB_URL>
```

Mode

Captive Portal Authentication

Description

Configure external captive portal vendor url.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
external-url http://192.168.168.1/external.html
```

Syntax

```
no external-url
```

Mode

Captive Portal Authentication

Description

Clear the external captive portal vendor url.

Example

```
no external-url
```

Syntax

```
welcome-url-source { custom | from-radius }
```

Mode

Captive Portal Authentication

Description

Configure captive portal welcome url source.

Options

custom Set custom type.

from-radius Set from radius type.

Example

```
welcome-url-source from-radius
```

Syntax

```
no welcome-url-source
```

Mode

Captive Portal Authentication

Description

Clear captive portal welcome url source.

Example

```
no welcome-url-source
```

Syntax

```
welcome-url <WEB_URL>
```

Mode

Captive Portal Authentication

Description

Configure custom captive portal welcome url.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
welcome-url http://192.168.168.1/welcome.html
```

Syntax

```
no welcome-url
```

Mode

Captive Portal Authentication

Description

Clear the custom captive portal welcome url.

Example

no welcome-url

Syntax

session-timeout-source { custom | from-radius }

Mode

Captive Portal Authentication

Description

Configure session timeout source.

Options

custom Set custom type.

from-radius Set from radius type.

Example

session-timeout-source from-radius

Syntax

no session-timeout-source

Mode

Captive Portal Authentication

Description

Clear session timeout source.

Example

no session-timeout-source

Syntax

session-timeout <UINT32> unit { days | hours | minutes }

Mode

Captive Portal Authentication

Description

Set session timeout for captive portal authentication.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

unit Set the session timeout in seconds.

- days*** Set the session timeout in days.
- hours*** Set the session timeout in hours.
- minutes*** Set the session timeout in minutes.

Example

```
session-timeout 15 unit minutes
```

Syntax

```
no session-timeout
```

Mode

Captive Portal Authentication

Description

Clear the custom session-timeout.

Example

```
no session-timeout
```

Syntax

```
idle-timeout-source { custom | from-radius }
```

Mode

Captive Portal Authentication

Description

Configure idle timeout source.

Options

- custom*** Set custom type.
- from-radius*** Set from radius type.

Example

```
idle-timeout-source from-radius
```

Syntax

```
no idle-timeout-source
```

Mode

Captive Portal Authentication

Description

Clear idle timeout source.

Example

```
no idle-timeout-source
```

Syntax

```
idle-timeout <UINT32> unit { days | hours | minutes }
```

Mode

Captive Portal Authentication

Description

Set idle timeout for captive portal authentication.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

unit Set the idle timeout in seconds.

days Set the idle timeout in days.

hours Set the idle timeout in hours.

minutes Set the idle timeout in minutes.

Example

```
idle-timeout 15 unit minutes
```

Syntax

```
no idle-timeout
```

Mode

Captive Portal Authentication

Description

Clear the custom idle-timeout.

Example

```
no idle-timeout
```

Syntax

```
method { chap | pap-cleartext | pap-encrypted }
```

Mode

Captive Portal Authentication

Description

Configure radius authentication method.

Options

chap Set chap type.

pap-cleartext Set pap-cleartext type.

pap-encrypted Set pap-encrypted type.

Example

```
method chap
```

Syntax

no method

Mode

Captive Portal Authentication

Description

Clear radius authentication method.

Example

no method

Syntax

enable

Mode

Policy Page Without Authentication

Description

Enable policy page without authentication.

Example

auto-accept

Syntax

no enable

Mode

Policy Page Without Authentication

Description

Disable policy page without authentication.

Example

no enable

Syntax

guest-usage-policy <WORD>

Mode

Policy Page Without Authentication

Description

Set custom login page which may include HTML formatting.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

guest-usage-policy "Welcome to Sonicwall."

Syntax

no guest-usage-policy

Mode

Policy Page Without Authentication

Description

Clear custom login page.

Example

no guest-usage-policy

Syntax

idle-timeout <UINT64> unit { *days* | *hours* | *minutes* | *seconds* }

Mode

Policy Page Without Authentication

Description

Set idle timeout for custom guest policy page.

Options

- <UINT64>** Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: *123*
- unit** Set the idle timeout in seconds.
- days** Set the idle timeout in days.
- hours** Set the idle timeout in hours.
- minutes** Set the idle timeout in minutes.
- seconds** Set the idle timeout in seconds.

Example

idle-timeout 15 unit minutes

Syntax

no idle-timeout

Mode

Policy Page Without Authentication

Description

Clear the custom idle-timeout.

Example

no idle-timeout

Syntax

auto-accept

Mode

Description

Enable auto accept policy page.

Example

```
auto-accept
```

Syntax

```
no auto-accept
```

Mode

Policy Page Without Authentication

Description

Disable auto accept policy page.

Example

```
no auto-accept
```

Syntax

```
custom-auth-page
```

Mode

Guest Services

Description

Enter its configuration mode.

Example

```
custom-auth-page
```

Syntax

```
post-auth <WEB_URL>
```

Mode

Guest Services

Description

Enable page to direct users to after successful authentication.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
post-auth http://192.168.168.1/postauth.html
```

Syntax

```
no post-auth
```


Mode

Guest Services

Description

Disable page to direct users to after successful authentication.

Example

no post-auth

Syntax

bypass-guest-auth { all | group <ADDR_MAC_GROUP> | mac <ADDR_MAC> | name <ADDR_MAC_NAME> }

Mode

Guest Services

Description

Enable bypass guest authentication.

Options

all	All MAC addresses.
group	Address group name.
<ADDR_MAC_GROUP>	MAC group address object name. Example: <i>Sales & Marketing Network Access Points</i>
mac	MAC address.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	MAC address object name.
<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>

Example

bypass-guest-auth mac 020102030405

Syntax

no bypass-guest-auth

Mode

Guest Services

Description

Disable bypass guest authentication.

Example

no bypass-guest-auth

Syntax

smtp-redirect { host <ADDR_HOST> | name <ADDR_HOST_NAME> }

Mode

Guest Services

Description

Enable redirect SMTP traffic to specified server.

Options

host	Set the SMTP server to host address.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Set the SMTP server as named address object.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

Example

smtp-redirect host 192.168.168.152

Syntax

no smtp-redirect

Mode

Guest Services

Description

Disable redirect SMTP traffic.

Example

no smtp-redirect

Syntax

deny-networks { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }

Mode

Guest Services

Description

Enable blocking of traffic to the named network.

Options

ipv6	IPv6 address object.
host	Set the denied networks to host address.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Set the denied networks to network address.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Set the denied networks to range of addresses.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_GROUP_NAME_MIXED>	Set the denied networks as named address group. Group address object name. Example: <i>Sales Group</i>
<i>mac</i> <ADDR_MAC>	Set the denied networks to MAC address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i> <ADDR_NAME_MIXED>	Set the denied networks as named address object. Address object name. Example: <i>Web Server</i>

Example

deny-networks network 192.168.168.0 255.255.255.0

Syntax

no deny-networks

Mode

Guest Services

Description

Disable blocking of traffic to the named network.

Example

no deny-networks

Syntax

pass-networks { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }

Mode

Guest Services

Description

Enable allowing of traffic to the named network.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i> <ADDR_HOST>	Set the pass networks to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i> <ADDR_NETWORK>	Set the pass networks to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <ADDR_BEGIN>	Set the pass networks to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form:

<ADDR_END>	HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Set the pass networks as named address group. Group address object name. Example: <i>Sales Group</i>
mac <ADDR_MAC>	Set the pass networks to MAC address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_MIXED>	Set the pass networks as named address object. Address object name. Example: <i>Web Server</i>

Example

```
pass-networks network 192.168.168.0 255.255.255.0
```

Syntax

```
no pass-networks
```

Mode

Guest Services

Description

Disable allowing of traffic to the named network.

Example

```
no pass-networks
```

Syntax

```
max-guests <UINT16>
```

Mode

Guest Services

Description

Specify the maximum number of guest users allowed to connect to the WLAN zone.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
 Example: *123*

Example

```
max-guests 10
```

Syntax

```
enable
```

Mode

Description

Enable custom authentication page.

Example

enable

Syntax

no enable

Mode

Custom Authentication Page

Description

Disable custom authentication page.

Example

no enable

Syntax

footer { text <WORD> | url <WEB_URL> }

Mode

Custom Authentication Page

Description

Configure custom login page footer.

Options

text	Use configured text for custom login page footer.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
url	Use configured url location for custom page footer.
<WEB_URL>	URL in the form: http://host/file. Example: <i>http://www.example.com/products/</i>

Example

footer url http://192.168.168.1/footer.html

Syntax

no footer

Mode

Custom Authentication Page

Description

Clear custom login page footer.

Example

no footer

Syntax

header { text <WORD> | url <WEB_URL> }

Mode

Custom Authentication Page

Description

Configure custom login page header.

Options

text	Use configured text for custom login page header.
<WORD>	Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i>
url	Use configured url location for custom login page header.
<WEB_URL>	URL in the form: http://host/file. Example: <i>http://www.example.com/products/</i>

Example

header url http://192.168.168.1/header.html

Syntax

no header

Mode

Custom Authentication Page

Description

Clear custom login page header.

Example

no header

Syntax

sslvpn-enforcement server { host <ADDR_HOST> | name <ADDR_HOST_NAME> } service { name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }

Mode

Wireless

Description

Enable SSLVPN enforcement.

Options

server	Set the SSLVPN server as a named address object.
host	Set the SSLVPN server to host address.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name	Set the SSLVPN server as named address object.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
service	Set the SSLVPN service as a named service object.

name	Set the SSLVPN service as named service object.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Set the SSLVPN service as a protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
sslvpn-enforcement server name "SSLVPN Server" service name "SSLVPN Service"
```

Syntax

```
no sslvpn-enforcement
```

Mode

Wireless

Description

Disable SSLVPN enforcement.

Example

```
no sslvpn-enforcement
```

Syntax

```
wifi-sec-enforcement [ exception-service { name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } ]
```

Mode

Wireless

Description

Enable WiFiSec enforcement.

Options

exception-service Specify services that are allowed to bypass wifisec enforcement.

name	Name of service object for the exception service.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Set the WiFiSec exception service as a protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
wifi-sec-enforcement
wifi-sec-enforcement service name "SSLVPN Service"
```

Syntax

```
no wifi-sec-enforcement [ exception-service ]
```

Mode

Wireless

Description

Disable WiFiSec enforcement.

Options

exception-service Disable WiFiSec enforcement exception service.

Example

```
no wifi-sec-enforcement
```

Syntax

```
wifi-sec-for-site-to-site-vpn
```

Mode

Wireless

Description

Enable WiFiSec for site-to-site VPN tunnel traversal.

Example

```
wifi-sec-for-site-to-site-vpn
```

Syntax

```
no wifi-sec-for-site-to-site-vpn
```

Mode

Wireless

Description

Disable WiFiSec for site-to-site VPN tunnel traversal.

Example

```
no wifi-sec-for-site-to-site-vpn
```

Syntax

```
trust-wpa-traffic-as-wifi-sec
```

Mode

Wireless

Description

Trust WPA / WPA2 traffic as WiFiSec.

Example

```
trust-wpa-traffic-as-wifi-sec
```

Syntax

```
no trust-wpa-traffic-as-wifi-sec
```

Mode

Wireless

Description

Disable trust WPA / WPA2 traffic as WiFiSec.

Example

```
no trust-wpa-traffic-as-wifi-sec
```

Syntax

```
sonicpoint profile { ac | n | ndr | wave2 } { auto-provisioning | profile-name <SONICPOINT_N_PROFILE_NAME> }
```

Mode

Wireless

Description

Set the sonicpoint provisioning profile.

Options

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2.
auto-provisioning	Enable auto provisioning sonicpoint profile.
profile-name	SonicPoint profile name.
<SONICPOINT_N_PROFILE_NAME>	SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i>

Example

```
sonicpoint profile n profile-name "Public SonicPointNs"  
sonicpoint profile n auto-provisioning
```

Syntax

```
no sonicpoint profile { ac | n | ndr | wave2 } auto-provisioning
```

Mode

Wireless

Description

Disable auto provisioning sonicpoint profile.

Options

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.

wave2 SonicPoint ACWave2.
auto-provisioning Disable auto provisioning sonicpoint profile.

Example

no sonicpoint profile n auto-provisioning

Syntax

bypass-gateway-firewalling

Mode

Wireless

Description

Enforce local wireless zone traffic to bypass gateway firewalling.

Example

bypass-gateway-firewalling

Syntax

no bypass-gateway-firewalling

Mode

Wireless

Description

Disable local wireless zone traffic to bypass gateway firewalling.

Example

no bypass-gateway-firewalling

Syntax

only-sonicpoint-traffic

Mode

Wireless

Description

Enable only allow traffic generated by a SonicPoint/SonicPointN.

Example

only-sonicpoint-traffic

Syntax

no only-sonicpoint-traffic

Mode

Wireless

Description

Disable only allow traffic generated by a SonicPoint/SonicPointN.

Example

```
no only-sonicpoint-traffic
```

Syntax

```
auto-channel-limitation
```

Mode

Wireless

Description

Enable prefer SonicPoint/SonicWave 2.4GHz auto channel selection to be 1, 6 and 11 only.

Example

```
auto-channel-limitation
```

Syntax

```
no auto-channel-limitation
```

Mode

Wireless

Description

Disable prefer SonicPoint/SonicWave 2.4GHz auto channel selection to be 1, 6 and 11 only.

Example

```
no auto-channel-limitation
```

Syntax

```
sonicwave-online-registration
```

Mode

Wireless

Description

Enable enforce SonicWave license activation from secure trusted license manager.

Example

```
sonicpoint-management
```

Syntax

```
no sonicwave-online-registration
```

Mode

Wireless

Description

Disable enforce SonicWave license activation from secure trusted license manager.

Example

no sonicwave-online-registration

Syntax

sonicpoint-management

Mode

Wireless

Description

Enable SonicPoint/SonicWave management.

Example

sonicpoint-management

Syntax

no sonicpoint-management

Mode

Wireless

Description

Disable SonicPoint/SonicWave management.

Example

no sonicpoint-management

Syntax

local-radius-server

Mode

Zone

Description

Enable zone local radius server and enter configuration mode.

Example

local-radius-server

Syntax

enable

Mode

Radius Server

Description

Enable zone local radius server.

Example

enable

Syntax

no enable

Mode

Radius Server

Description

Disable zone local radius server.

Example

no enable

Syntax

interface-server-numbers <UINT16>

Mode

Radius Server

Description

Specify the interface server numbers.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

interface-server-numbers 8

Syntax

port <UINT32>

Mode

Radius Server

Description

Set radius server port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

port 1812

Syntax

client-password <ENC_PASSWORD>

Mode

Radius Server

Description

Set radius client password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

client-password mywpapassphrase

Syntax

no client-password

Mode

Radius Server

Description

Clear radius client password.

Example

no client-password

Syntax

tls-cache

Mode

Radius Server

Description

Enable local radius server tls cache.

Example

tls-cache

Syntax

no tls-cache

Mode

Radius Server

Description

Disable local radius server tls cache.

Example

no tls-cache

Syntax

tls-cache-lifetime <UINT8>

Mode

Radius Server

Description

Specify the radius server tls cache lifetime(h).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
tls-cache-lifetime 1
```

Syntax

```
ldap-server
```

Mode

Radius Server

Description

Enable zone ldap server and enter configuration mode.

Example

```
ldap-server
```

Syntax

```
enable
```

Mode

LDAP Server

Description

Enable ldap server.

Example

```
server 192.168.168.1
```

Syntax

```
no enable
```

Mode

LDAP Server

Description

Disable ldap server.

Example

```
no server
```

Syntax

```
server <HOSTNAME>
```

Mode

LDAP Server

Description

Specify the ldap server name or ip.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
server 192.168.168.1
```

Syntax

```
no server
```

Mode

LDAP Server

Description

Clear the ldap server name or ip.

Example

```
no server
```

Syntax

```
base-dn <WORD>
```

Mode

LDAP Server

Description

Specify the ldap server base dn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
base-dn "ou=radius,dc=sonicwall,dc=com"
```

Syntax

```
no base-dn
```

Mode

LDAP Server

Description

Clear the ldap server base dn.

Example

```
no base-dn
```

Syntax

identity-dn <WORD>

Mode

LDAP Server

Description

Specify the ldap server identity dn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

identity-dn "cn=snwlradius,ou=admins,ou=radius,dc=sonicwall,dc=com"

Syntax

no identity-dn

Mode

LDAP Server

Description

Clear the ldap server identity dn.

Example

no identity-dn

Syntax

identity-dn-password <ENC_PASSWORD>

Mode

LDAP Server

Description

Set ldap identity dn password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

identity-dn-password mypassphrase

Syntax

no identity-dn-password

Mode

LDAP Server

Description

Clear ldap identity dn password.

Example

```
no identity-dn-password
```

Syntax

```
tls
```

Mode

LDAP Server

Description

Enable ldap server tls.

Example

```
tls
```

Syntax

```
no tls
```

Mode

LDAP Server

Description

Disable ldap server tls.

Example

```
no tls
```

Syntax

```
cache
```

Mode

LDAP Server

Description

Enable ldap cache.

Example

```
cache
```

Syntax

```
no cache
```

Mode

LDAP Server

Description

Disable ldap server cache.

Example

```
no cache
```

Syntax

cache-lifetime <UINT32>

Mode

LDAP Server

Description

Specify the ldap server cache lifetime(s).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

cache-lifetime 86400

Syntax

active-directory-server

Mode

Radius Server

Description

Enable zone active directory server and enter configuration mode.

Example

active-directory-server

Syntax

enable

Mode

Active Directory Server

Description

Enable active directory.

Example

enable

Syntax

no enable

Mode

Active Directory Server

Description

Disable active directory.

Example

no enable

Syntax

domain <HOSTNAME>

Mode

Active Directory Server

Description

Specify the active directory server domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

domain wirelessdev

Syntax

no domain

Mode

Active Directory Server

Description

Clear the active directory server domain.

Example

no domain

Syntax

full-name <WORD>

Mode

Active Directory Server

Description

Specify the active directory server full name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

full-name wirelessdev.com

Syntax

no full-name

Mode

Active Directory Server

Description

Clear the active directory server full name.

Example

```
no domain
```

Syntax

```
admin-user-name <WORD>
```

Mode

Active Directory Server

Description

Specify the active directory server admin user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
admin-user-name wirelessDev
```

Syntax

```
no admin-user-name
```

Mode

Active Directory Server

Description

Clear the active directory server admin user name.

Example

```
no admin-user-name
```

Syntax

```
admin-user-password <ENC_PASSWORD>
```

Mode

Active Directory Server

Description

Set active directory server admin user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
admin-user-password mypassphrase
```

Syntax

```
no admin-user-password
```

Mode

Active Directory Server

Description

Clear active directory server admin user password.

Example

```
no admin-user-password
```

Syntax

```
no packet-dissection-object <PDF_NAME>
```

Mode

Config

Description

Delete a packet dissection object.

Options

<PDF_NAME> Packet Dissection object name.
Example: *PdfName*

Example

```
no packet-dissection-object "Corp Address"
```

Syntax

```
no packet-dissection-objects
```

Mode

Config

Description

Delete all custom packet dissection objects.

Example

```
no packet-dissection-objects
```

Syntax

```
packet-dissection-object <PDF_NAME>
```

Mode

Config

Description

Add/edit packet dissection object and enter configuration mode.

Options

<PDF_NAME> Packet Dissection object name.
Example: *PdfName*

Example

```
packet-dissection-object "Corp Address"
```

Syntax

```
no packet-dissection-group <PDF_GROUP_NAME>
```

Mode

Config

Description

Delete a packet dissection group.

Options

<PDF_GROUP_NAME> Packet Dissection Group name.
Example: PdfGroupName

Example

```
no packet-dissection-group "Corporate Dissection Group"
```

Syntax

```
no packet-dissection-groups
```

Mode

Config

Description

Delete all custom packet dissection groups.

Example

```
no packet-dissection-groups
```

Syntax

```
packet-dissection-group <PDF_GROUP_NAME>
```

Mode

Config

Description

Add/edit packet dissection group and enter configuration mode.

Options

<PDF_GROUP_NAME> Packet Dissection Group name.
Example: PdfGroupName

Example

```
packet-dissection-group "Corporate Dissection Group"
```

Syntax

```
name <PDF_GROUP_NAME>
```

Mode

Packet Dissection Group

Description

Set packet dissection group name.

Options

<PDF_GROUP_NAME> Packet Dissection Group name.
Example: *PdfGroupName*

Example

name "Corporate Dissection Group "

Syntax

negative-matching

Mode

Packet Dissection Group

Description

Enable negative matching.

Example

negative-matching

Syntax

no negative-matching

Mode

Packet Dissection Group

Description

Disable negative matching.

Example

no negative-matching

Syntax

match-type { all | any }

Mode

Packet Dissection Group

Description

Set the packet dissection group to match given parameter.

Options

all All.

any Any.

Example

match-type any

Syntax

no packet-dissection-object <PDF_NAME>

Mode

Packet Dissection Group

Description

Remove packet dissection object from group.

Options

<PDF_NAME> Packet Dissection object name.
Example: *PdfName*

Example

no packet-dissection-object "Corp E-mail Server"

Syntax

no packet-dissection-objects

Mode

Packet Dissection Group

Description

Remove all packet dissection objects from group.

Example

no packet-dissection-objects

Syntax

packet-dissection-object <PDF_NAME>

Mode

Packet Dissection Group

Description

Assign packet dissection object to group.

Options

<PDF_NAME> Packet Dissection object name.
Example: *PdfName*

Example

packet-dissection-object "Corp E-mail Server"

Syntax

no packet-dissection-group <PDF_GROUP_NAME>

Mode

Packet Dissection Group

Description

Remove packet dissection group from group.

Options

<PDF_GROUP_NAME> Packet Dissection Group name.
Example: *PdfGroupName*

Example

```
no packet-dissection-group "Corp Web Servers"
```

Syntax

```
no packet-dissection-groups
```

Mode

Packet Dissection Group

Description

Remove all packet dissection groups from group.

Example

```
no packet-dissection-groups
```

Syntax

```
packet-dissection-group <PDF_GROUP_NAME>
```

Mode

Packet Dissection Group

Description

Assign packet dissection group to group.

Options

<PDF_GROUP_NAME> Packet Dissection Group name.
Example: *PdfGroupName*

Example

```
packet-dissection-group "Corp Web Servers"
```

Syntax

```
name <PDF_NAME>
```

Mode

Packet Dissection Object

Description

Set packet dissection object name.

Options

<PDF_NAME> Packet Dissection object name.
Example: *PdfName*

Example

```
name "Corp E-mail Server "
```

Syntax

```
negative-matching
```

Mode

Packet Dissection Object

Description

Enable negative matching.

Example

```
negative-matching
```

Syntax

```
no negative-matching
```

Mode

Packet Dissection Object

Description

Disable negative matching.

Example

```
no negative-matching
```

Syntax

```
family ipv4 { flag | fragment-offset | header-checksum | header-length | identity | option-type | packet-length | protocol | ttl | version }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

flag	IPv4 header with header field flag.
fragment-offset	IPv4 header with header field fragment offset.
header-checksum	IPv4 header with header field header checksum.
header-length	IPv4 header with header field header length.
identity	IPv4 header with header field identity.
option-type	IPv4 header with header field option type.
packet-length	IPv4 header with header field packet length.
protocol	IPv4 header with header field protocol.

<i>ttl</i>	IPv4 header with header field TTL.
<i>version</i>	IPv4 header with header field IPv4 Version.

Example

```
family ipv4 version
```

Syntax

```
family ipv6 { flow-label | fragment-offset | home-address-options | hop-limit | next-header | payload-length | routing-header-length | routing-header-segments-left | routing-header-type | traffic-class | version }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

<i>flow-label</i>	IPv6 header with header field IPv6 flow label.
<i>fragment-offset</i>	IPv6 header with header field fragment offset.
<i>home-address-options</i>	IPv6 header with header field IPv6 home address options.
<i>hop-limit</i>	IPv6 header with header IPv6 hop limit.
<i>next-header</i>	IPv6 header with header field IPv6 next header.
<i>payload-length</i>	IPv6 header with header field IPv6 payload length.
<i>routing-header-length</i>	IPv6 header with header field IPv6 routing header length.
<i>routing-header-segments-left</i>	IPv6 header with header field IPv6 routing header segments left.
<i>routing-header-type</i>	IPv6 header with header field IPv6 routing header type.
<i>traffic-class</i>	IPv6 header with header field IPv6 traffic class.
<i>version</i>	IPv6 header with header field IPv6 Version.

Example

```
family ipv4 version
```

Syntax

```
family icmpv4 { checksum | code | gateway-address | identifier | orig-timestamp | param-problem-pointer | recv-timestamp | sequence | trans-timestamp | type }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

<i>checksum</i>	ICMPv4 header with header field checksum.

<i>code</i>	ICMPv4 header with header field code.
<i>gateway-address</i>	ICMPv4 header with header field gateway address.
<i>identifier</i>	ICMPv4 header with header field identifier.
<i>orig-timestamp</i>	ICMPv4 header with header field orig timestamp.
<i>param-problem-pointer</i>	ICMPv4 header with header field para problem pointer.
<i>recv-timestamp</i>	ICMPv4 header with header recv timestamp.
<i>sequence</i>	ICMPv4 header with header field sequence.
<i>trans-timestamp</i>	ICMPv4 header with header field trans timestamp.
<i>type</i>	ICMPv4 header with header field type.

Example

```
family icmpv4 checksum
```

Syntax

```
family icmpv6 { checksum | code | type }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

checksum ICMPv6 header with header field checksum.

code ICMPv6 header with header field code.

type ICMPv6 header with header field type.

Example

```
family icmpv6 checksum
```

Syntax

```
family tcp { ack-number | checksum | data-offset | flag | header-length | mss | packet-length | reserved | sequence-number |
urgent-pointer | window | window-scale }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

ack-number TCP header with header field ACK number.

checksum TCP header with header field tcp checksum.

<i>data-offset</i>	TCP header with header data offset.
<i>flag</i>	TCP header with header field flag.
<i>header-length</i>	TCP header with header field header length.
<i>mss</i>	TCP header with header field option - MSS.
<i>packet-length</i>	TCP header with header field packet length.
<i>reserved</i>	TCP header with header field reserved.
<i>sequence-number</i>	TCP header with header field sequence number.
<i>urgent-pointer</i>	TCP header with header field urgent pointer.
<i>window</i>	TCP header with header field window.
<i>window-scale</i>	TCP header with header field option - window scale.

Example

```
family tcp checksum
```

Syntax

```
family udp { checksum | packet-length }
```

Mode

Packet Dissection Object

Description

Set the packet dissection object family and header field.

Options

<i>checksum</i>	UDP header with header field udp checksum.
<i>packet-length</i>	UDP header with header field packet length.

Example

```
family udp checksum
```

Syntax

```
reserved
```

Mode

Packet Dissection IPV4 bitset

Description

Enable reserved in bitset.

Example

```
reserved
```

Syntax

no reserved

Mode

Packet Dissection IPV4 bitset

Description

Disable reserved in bitset.

Example

no reserved

Syntax

dont-fragment

Mode

Packet Dissection IPV4 bitset

Description

Enable dont-fragment in bitset.

Example

dont-fragment

Syntax

no dont-fragment

Mode

Packet Dissection IPV4 bitset

Description

Disable dont-fragment in bitset.

Example

no dont-fragment

Syntax

more-fragments

Mode

Packet Dissection IPV4 bitset

Description

Enable more-fragments in bitset.

Example

more-fragments

Syntax

no more-fragments

Mode

Packet Dissection IPV4 bitset

Description

Disable more-fragments in bitset.

Example

```
no more-fragments
```

Syntax

```
fin
```

Mode

Packet Dissection TCP bitset

Description

Enable FIN in bitset.

Example

```
fin
```

Syntax

```
no fin
```

Mode

Packet Dissection TCP bitset

Description

Disable FIN in bitset.

Example

```
no fin
```

Syntax

```
syn
```

Mode

Packet Dissection TCP bitset

Description

Enable SYN in bitset.

Example

```
syn
```

Syntax

```
no syn
```

Mode

Packet Dissection TCP bitset

Description

Disable SYN in bitset.

Example

```
no syn
```

Syntax

```
rst
```

Mode

Packet Dissection TCP bitset

Description

Enable RST in bitset.

Example

```
rst
```

Syntax

```
no rst
```

Mode

Packet Dissection TCP bitset

Description

Disable RST in bitset.

Example

```
no rst
```

Syntax

```
push
```

Mode

Packet Dissection TCP bitset

Description

Enable PUSH in bitset.

Example

```
push
```

Syntax

```
no push
```

Mode

Packet Dissection TCP bitset

Description

Disable PUSH in bitset.

Example

no push

Syntax

ack

Mode

Packet Dissection TCP bitset

Description

Enable ACK in bitset.

Example

ack

Syntax

no ack

Mode

Packet Dissection TCP bitset

Description

Disable ACK in bitset.

Example

no ack

Syntax

urg

Mode

Packet Dissection TCP bitset

Description

Enable URG in bitset.

Example

urg

Syntax

no urg

Mode

Packet Dissection TCP bitset

Description

Disable URG in bitset.

Example

no urg

Syntax
<i>ece</i>
Mode
Packet Dissection TCP bitset
Description
Enable ECE in bitset.
Example
<i>ece</i>

Syntax
<i>no ece</i>
Mode
Packet Dissection TCP bitset
Description
Disable ECE in bitset.
Example
<i>no ece</i>

Syntax
<i>cwr</i>
Mode
Packet Dissection TCP bitset
Description
Enable CWR in bitset.
Example
<i>cwr</i>

Syntax
<i>no cwr</i>
Mode
Packet Dissection TCP bitset
Description
Disable CWR in bitset.
Example
<i>no cwr</i>

Syntax

```
data-type [ hex <WORD> | ipv4-address <IPV4_HOST> | ipv4-bitset | ipv4-range <IPV4_HOST> <IPV4_HOST> | ipv6-address <IPV6_HOST> | ipv6-range <IPV6_HOST> <IPV6_HOST> | numeric <UINT64> | range <UINT64> <UINT64> | range-hex <WORD> <WORD> | tcp-bitset ]
```

Mode

Packet Dissection Object

Description

Set the packet dissection data type.

Options

hex	Numeric(hex).
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
ipv4-address	IPv4 address.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
ipv4-bitset	IPv4 bitset.
ipv4-range	IPv4 range.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
ipv6-address	IPv6 address.
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
ipv6-range	IPv6 range.
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
numeric	Numeric data type
<UINT64>	Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH. Example: <i>123</i>
range	Range of values.
<UINT64>	Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH. Example: <i>123</i>
<UINT64>	Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH. Example: <i>123</i>
range-hex	Range(hex).
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
tcp-bitset	TCP bitset.

Example

```
data-type ipv4-address 10.10.10.10
```

Syntax

```
show address-objects [ fqdn | ipv4 [ { host | network | range } ] | ipv6 [ { host | network | range } ] | mac ] [ { custom | default } ] [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all address objects.

Options

<i>fqdn</i>	Show FQDN address objects.
<i>ipv4</i>	Show only IPv4 address objects.
<i>host</i>	Show host address objects.
<i>network</i>	Show network address objects.
<i>range</i>	Show range address objects.
<i>ipv6</i>	Show only IPv6 address objects.
<i>host</i>	Show host address objects.
<i>network</i>	Show network address objects.
<i>range</i>	Show range address objects.
<i>mac</i>	Show MAC address objects.
<i>custom</i>	Show custom configuration.
<i>default</i>	Show system/factory default configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show address object status.

Example

show address-objects

Syntax

show address-object ipv4 [uuid] <ADDR_HOST_NETWORK_RANGE_NAME> [{ pending-config | with-pending-config }] [status]

Mode

All Modes

Description

Show an IPv4 address object.

Options

<i>uuid</i>	Show an IPv4 address object by UUID.
<i><ADDR_HOST_NETWORK_RANGE_NAME></i>	Host/network/range address object name. Example: <i>Web Server</i>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show address object status.

Example

show address-object ipv4 "X0 IP"

Syntax

```
show address-object ipv6 [ uuid ] <ADDR_HOST_NETWORK_RANGE_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an IPv6 address object.

Options

uuid	Show an IPv6 address object by UUID.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show address object status.

Example

```
show address-object ipv6 "X0 IPv6 Link-Local Address"
```

Syntax

```
show address-object mac [ uuid ] <ADDR_MAC_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show a MAC address object.

Options

uuid	Show a MAC address object by UUID.
<ADDR_MAC_NAME>	MAC address object name. Example: <i>Sales Network Access Point</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show address object status.

Example

```
show address-object mac "Web Server MAC"
```

Syntax

```
show address-object fqdn [ uuid ] <ADDR_FQDN_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show a FQDN address object.

Options

uuid	Show an FQDN address object by UUID.
<ADDR_FQDN_NAME>	FQDN address object name.

Example: *www.example.com*

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show address object status.

Example

```
show address-object fqdn "Web Server FQDN"
```

Syntax

```
show address-groups [ ipv4 | ipv6 ] [ { custom | default } ] [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all address groups.

Options

<i>ipv4</i>	Show only IPv4 address groups.
<i>ipv6</i>	Show only IPv6 address groups.
<i>custom</i>	Show custom configuration.
<i>default</i>	Show system/factory default configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show address group status.

Example

```
show address-groups
```

Syntax

```
show address-group ipv4 [ uuid ] <ADDR_GROUP_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an address group.

Options

<i>uuid</i>	Show an IPv4 address group by UUID.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show address group status.

Example

```
show address-group ipv4 "LAN Subnets"
```

Syntax

```
show address-group ipv6 [ uuid ] <ADDR_GROUP_NAME> [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show an address group.

Options

uuid	Show an IPv6 address group by UUID.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show address group status.

Example

```
show address-group ipv6 "DMZ IPv6 Subnets"
```

Syntax

```
show schedules [ all | mixed | once | recurring | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all schedule objects.

Options

all	Show all schedule objects.
mixed	Show all schedule objects set for both recurring schedule and single occurrence.
once	Show all schedule objects set for single occurrence.
recurring	Show all schedule objects set for recurring.
status	Show all schedule objects status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show schedules
```

Syntax

```
show schedule [ uuid ] <SCHED_NAME> [ { pending-config | with-pending-config } ]
```


Mode

All Modes

Description

Show a schedule object.

Options

uuid	Show a schedule object by UUID.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show schedule "Work Hours"

Syntax

show service-objects [6over4 | ah | eigrp | esp | gre | icmp | icmpv6 | igmp | l2tp | ospf | pim | tcp | udp] [{ pending-config | with-pending-config }] [status]

Mode

All Modes

Description

Show all service objects.

Options

6over4	Show 6over4 service objects.
ah	Show AH service objects.
eigrp	Show EIGRP service objects.
esp	Show ESP service objects.
gre	Show GRE service objects.
icmp	Show ICMP service objects.
icmpv6	Show ICMPV6 service objects.
igmp	Show IGMP service objects.
l2tp	Show l2tp service objects.
ospf	Show OSPF service objects.
pim	Show PIM service objects.
tcp	Show TCP service objects.
udp	Show UDP service objects.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show service object status.

Example

```
show service-objects
```

Syntax

```
show service-object [ uuid ] <SVC_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show service object.

Options

- uuid** Show a service object by UUID.
- <SVC_NAME>** Service object name.
Example: *HTTPS*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show service-object "Corp Servers"
```

Syntax

```
show service-groups [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all service groups.

Options

- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.
- status** Show service group status.

Example

```
show service-groups
```

Syntax

```
show service-group [ uuid ] <SVC_GROUP_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show service group.

Options

uuid	Show a sevice group by UUID.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show service-group "Citrix"
```

Syntax

```
show zones [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all Zone Objects.

Options

status	Show zones status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show zones
```

Syntax

```
show zone [ uuid ] <ZONE_NAME> [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a Zone Object.

Options

uuid	Show a zone object by UUID.
<ZONE_NAME>	Zone object name. Example: <i>DMZ</i>
status	Show zone status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show zone "LAN"
```

Syntax

```
show packet-dissection-object <PDF_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show packet dissection object.

Options

- <PDF_NAME>** Packet Dissection object name.
Example: *PdfName*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

show packet-dissection-object "Corp Servers"

Syntax

show packet-dissection-objects [{ pending-config | with-pending-config }] [status]

Mode

All Modes

Description

Show all packet dissection objects.

Options

- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.
- status** Show packet dissection object status.

Example

show packet-dissection-objects

Syntax

show packet-dissection-group <PDF_GROUP_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show packet dissection group.

Options

- <PDF_GROUP_NAME>** Packet Dissection Group name.
Example: *PdfGroupName*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

show packet-dissection-group "Corp Dissection Group"

Syntax

```
show packet-dissection-groups [ { pending-config | with-pending-config } ] [ status ]
```

Mode

All Modes

Description

Show all packet dissection groups.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show packet dissection group status.

Example

```
show packet-dissection-groups
```

Syntax

```
clear interface [ ipv4 | ipv6 ] statistics
```

Mode

All Modes
Top Level

Description

Reset interface statistics.

Options

<i>ipv4</i>	Reset interface IPv4 statistics.
<i>ipv6</i>	Reset interface IPv6 statistics.
<i>statistics</i>	Reset interface statistics.

Example

```
clear interface statistics
```

Syntax

```
interface-statistics display-all-traffic
```

Mode

Config

Description

Enable display all traffic.

Example

```
interface-statistics display-all-traffic
```

Syntax

```
no interface-statistics display-all-traffic
```

Mode

Config

Description

Disable display all traffic.

Example

```
no interface-statistics display-all-traffic
```

Syntax

```
shutdown <CONFIGURABLE_INTERFACE>
```

Mode

Config

Description

Shutdown specified port.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
shutdown X2
```

Syntax

```
no shutdown <CONFIGURABLE_INTERFACE>
```

Mode

Config

Description

Enable specified port.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
no shutdown X2
```

Syntax

```
interface [ ipv6 ] <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ]
```

Mode

Config

Description

Configure interface or add/edit sub-interface or WLAN tunnel interface.

Options

ipv6	Configure interface IPv6 parameters.
<CONFIGURABLE_INTERFACE>	Interface name. Example: <i>X0</i>
vlan	Configure VLAN sub-interface.
<VLAN_TAG>	VLAN tag. Example: <i>23</i>
tunnel	Configure WLAN tunnel interface.
<WLAN_TUNNEL_ID>	WLAN tunnel ID. Example: <i>1</i>

Example

```
interface X1
interface X1 vlan 100
interface WT0
interface X1 tunnel 1
interface X1 vlan 100 tunnel 2
interface WT1 vlan 200
interface ipv6 X1
interface ipv6 X1 vlan 100
interface ipv6 WT0
interface ipv6 X1 tunnel 1
interface ipv6 X1 vlan 100 tunnel 2
interface ipv6 WT1 vlan 200
```

Syntax

```
no interface <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ]
```

Mode

Config

Description

Delete sub-interface or WLAN tunnel interface.

Options

<CONFIGURABLE_INTERFACE>	Interface name. Example: <i>X0</i>
vlan	Delete VLAN sub-interface.
<VLAN_TAG>	VLAN tag. Example: <i>23</i>
tunnel	Delete WLAN tunnel interface.
<WLAN_TUNNEL_ID>	WLAN tunnel ID. Example: <i>1</i>

Example

```
no interface X1 vlan 101
no interface WT0
no interface WT1 vlan 100
no interface X1 tunnel 1
no interface X1 vlan 101 tunnel 2
```

Syntax

```
no interfaces vlan
```

Mode

Config

Description

Delete all VLAN interfaces.

Example

```
no interfaces vlan
```

Syntax

no interfaces tunnel

Mode

Config

Description

Delete all WLAN tunnel interfaces.

Example

no interface tunnel

Syntax

tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE>

Mode

Config

Description

Add/edit 4to6 tunnel interface.

Options

<TUNNEL6_TUNNEL_INTERFACE> Tunnel6 tunnel interface name.
Example: *tunnel6TunnelInterface*

Example

tunnel-interface 4to6 CorpTunnel6Tunnel

Syntax

no tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE>

Mode

Config

Description

Delete 4to6 tunnel interface.

Options

<TUNNEL6_TUNNEL_INTERFACE> Tunnel6 tunnel interface name.
Example: *tunnel6TunnelInterface*

Example

no tunnel-interface 4to6 CorpTunnel6Tunnel

Syntax

no tunnel-interfaces 4to6

Mode

Config

Description

Delete all 4to6 tunnel interfaces.

Example

```
no tunnel-interfaces 4to6
```

Syntax

```
name <TUNNEL6_TUNNEL_INTERFACE>
```

Mode

Tunnel6 Tunnel Interface

Description

Set 4to6 tunnel interface name.

Options

<TUNNEL6_TUNNEL_INTERFACE> Tunnel6 tunnel interface name.
Example: *tunnel6TunnelInterface*

Example

```
name 4to6Tunnel
```

Syntax

```
comment <WORD>
```

Mode

Tunnel6 Tunnel Interface

Description

Set 4to6 tunnel interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Tunnel6 tunnel to Corporate"
```

Syntax

```
no comment
```

Mode

Tunnel6 Tunnel Interface

Description

Clear tunnel interface comment.

Example

```
no comment
```

Syntax

flow-reporting

Mode

Tunnel6 Tunnel Interface

Description

Enable flow reporting on the interface.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Tunnel6 Tunnel Interface

Description

Disable flow reporting on the interface.

Example

no flow-reporting

Syntax

send-icmp-fragmentation

Mode

Tunnel6 Tunnel Interface

Description

Enable send ICMP Fragmentation Needed for outbound packets over the Interface MTU.

Example

send-icmp-fragmentation

Syntax

no send-icmp-fragmentation

Mode

Tunnel6 Tunnel Interface

Description

Disable ICMP fragmentation needed message generation.

Example

no send-icmp-fragmentation

Syntax

fragment-packets

Mode

Tunnel6 Tunnel Interface

Description

Enable fragment non-VPN outbound packets larger than this interface's MTU.

Example

```
fragment-packets
```

Syntax

```
no fragment-packets
```

Mode

Tunnel6 Tunnel Interface

Description

Disable fragment non-VPN outbound packets larger than this interface's MTU.

Example

```
no fragment-packets
```

Syntax

```
ignore-df-bit
```

Mode

Tunnel6 Tunnel Interface

Description

Enable ignore don't fragment (DF) bit.

Example

```
ignore-df-bit
```

Syntax

```
no ignore-df-bit
```

Mode

Tunnel6 Tunnel Interface

Description

Disable ignore don't fragment (DF) bit.

Example

```
no ignore-df-bit
```

Syntax

```
type { dslite | gre4to6 }
```

Mode

Tunnel6 Tunnel Interface

Description

Set the tunnel interface tunnel6 type.

Options

dslite Dslite tunnel.

gre4to6 gre4to6 tunnel.

Example

type ds-lite

Syntax

bound-to interface <TUNNEL6_TUNNEL_BOUND_TO_INTERFACE>

Mode

ds-lite Tunnel Interface

Description

Set ds-lite software tunnel interface bound to.

Options

<TUNNEL6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

bound-to interface X1

Syntax

no bound-to

Mode

ds-lite Tunnel Interface

Description

Clear ds-lite software tunnel interface bound to.

Example

no bound-to

Syntax

bound-to interface <TUNNEL6_TUNNEL_BOUND_TO_INTERFACE>

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface bound to.

Options

<TUNNEL6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

bound to interface X1

Syntax

no bound-to

Mode

6to4 Tunnel Interface

Description

Clear gre4to6 tunnel interface bound to.

Example

no bound-to

Syntax

local { dynamic | ipv6 <IPV6_HOST> }

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface local IPv6 address.

Options

- dynamic** Set dslite tunnel interface primary local IPv6 address.
- ipv6** Set dslite tunnel interface static local IPv6 address.
- <IPV6_HOST>** IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

local ipv6 1030::C9B4:FF12:48AA:1A2B

Syntax

remote { dynamic | fqdn <WORD> | ipv6 <IPV6_HOST> }

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface remote IPv6 address.

Options

- dynamic** Set dslite tunnel interface remote IPv6 address via DHCP.
- fqdn** Set dslite tunnel interface static remote IPv6 address via FQDN
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- ipv6** Set dslite tunnel interface static remote IPv6 address.
- <IPV6_HOST>** IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.

Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
remote ipv6 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
local-ipv4 <IPv4_HOST>
```

Mode

dslite Tunnel Interface

Description

Set dslite tunnel interface local IPv4 address.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
local-ipv4 10.10.10.10
```

Syntax

```
no local-ipv4
```

Mode

dslite Tunnel Interface

Description

Clear dslite tunnel interface local IPv4 address.

Example

```
no local-ipv4
```

Syntax

```
remote ipv6 <IPv6_HOST>
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface remote IPv6 address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
remote 1030::C9B4:FF12:48AA:1A2B
```

Syntax

no remote

Mode

6to4 Tunnel Interface

Description

Clear gre4to6 tunnel interface remote IPv6 address.

Example

no remote

Syntax

```
local { dynamic | ipv6 <IPV6_HOST> }
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface local IPv6 address.

Options

<i>dynamic</i>	Set gre4to6 tunnel interface primary local IPv6 address.
<i>ipv6</i>	Set gre4to6 tunnel interface static local IPv6 address.
<i><IPV6_HOST></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
local ip 1030::C9B4:FF12:48AA:1A2B
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

6to4 Tunnel Interface

Description

Set gre4to6 tunnel interface IP address.

Options

<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>netmask</i>	Set interface netmask.
<i><IPV4_MASK></i>	IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: <i>255.255.255.0</i>

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

Description

Clear gre4to6 tunnel interface IP address.

Example

```
no ip
```

Syntax

```
tunnel-interface vpn <VPN_TUNNEL_INTERFACE>
```

Mode

Config

Description

Add/edit VPN tunnel interface.

Options

<VPN_TUNNEL_INTERFACE> VPN tunnel interface name.
Example: *vpnTunnelInterface*

Example

```
tunnel-interface vpn CorpVPNTunnel
```

Syntax

```
no tunnel-interface vpn <VPN_TUNNEL_INTERFACE>
```

Mode

Config

Description

Delete VPN tunnel interface.

Options

<VPN_TUNNEL_INTERFACE> VPN tunnel interface name.
Example: *vpnTunnelInterface*

Example

```
no tunnel-interface vpn CorpVPNTunnel
```

Syntax

```
no tunnel-interfaces vpn
```

Mode

Config

Description

Delete all VPN tunnel interface.

Example

```
no tunnel-interfaces vpn
```

Syntax

```
policy <VPN_TUNNEL_POLICY_NAME>
```

Mode

Tunnel Interface VPN

Description

Set tunnel interface VPN policy.

Options

<VPN_TUNNEL_POLICY_NAME> Tunnel interface VPN policy name.
Example: *Remote Office*

Example

```
policy "Remote Office"
```

Syntax

```
renew [ ipv6 ] <DHCP_INTERFACE>
```

Mode

Config

Description

Renew interface DHCP lease.

Options

ipv6 Renew interface DHCPv6 lease.
<DHCP_INTERFACE> Interface name.
Example: *X0*

Example

```
renew X5
```

Syntax

```
release [ ipv6 ] <DHCP_INTERFACE>
```

Mode

Config

Description

Release designated interface DHCP lease.

Options

ipv6 Release interface DHCPv6 lease.
<DHCP_INTERFACE> Interface name.
Example: *X0*

Example

```
release X5
```

Syntax

```
connect <CONNECT_INTERFACE>
```

Mode

Config

Description

Connect designated interface to PPTP/L2TP/PPPoE server.

Options

<CONNECT_INTERFACE> Interface name.
Example: *X0*

Example

connect X5

Syntax

disconnect <CONNECT_INTERFACE>

Mode

Config

Description

Disconnect designated interface from PPTP/L2TP/PPPoE server.

Options

<CONNECT_INTERFACE> Interface name.
Example: *X0*

Example

disconnect X5

Syntax

link-speed { auto-negotiate | full { { 10 | 100 | 1000 | 10000 | 100000 | 2500 | 40000 | 5000 } } | half { { 10 | 100 } } }

Mode

Interface

Description

Set interface link speed.

Options

- auto-negotiate*** Set interface link speed to auto-negotiate.
- full*** Full duplex.
- 10*** Set interface link speed to 10 Mbps-full duplex.
- 100*** Set interface link speed to 100 Mbps-full duplex.
- 1000*** Set interface link speed to 1000 Mbps-full duplex.
- 10000*** Set interface link speed to 10 Gbps(10000 Mbps)-full duplex.
- 100000*** Set interface link speed to 100 Gbps(100000 Mbps)-full duplex.
- 2500*** Set interface link speed to 2500 Mbps-full duplex.

<i>40000</i>	Set interface link speed to 40 Gbps(40000 Mbps)-full duplex.
<i>5000</i>	Set interface link speed to 5000 Mbps-full duplex.
<i>half</i>	Half duplex.
<i>10</i>	Set interface link speed to 10 Mbps-half duplex.
<i>100</i>	Set interface link speed to 100 Mbps-half duplex.

Example

```
link-speed half 100
```

Syntax

```
comment <WORD>
```

Mode

Interface
Tunnel Interface VPN

Description

Set interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Interface X0"
```

Syntax

```
no comment
```

Mode

Interface
Tunnel Interface VPN

Description

Clear interface comment.

Example

```
no comment
```

Syntax

```
bandwidth-management egress <DECIMAL>
```

Mode

Interface

Description

Enable and set egress bandwidth management in Kbps.

Options

<DECIMAL> Decimal in the form: n+.n+.

Example: 0.999

Example

```
bandwidth-management egress 1000
```

Syntax

```
no bandwidth-management egress
```

Mode

Interface

Description

Disable egress bandwidth management.

Example

```
no bandwidth-management egress
```

Syntax

```
bandwidth-management ingress <DECIMAL>
```

Mode

Interface

Description

Enable and set ingress bandwidth management in Kbps.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
bandwidth-management ingress 1000
```

Syntax

```
no bandwidth-management ingress
```

Mode

Interface

Description

Disable ingress bandwidth management.

Example

```
no bandwidth-management ingress
```

Syntax

```
send-icmp-fragmentation
```

Mode

Interface

Description

Enable ICMP fragmentation needed message generation.

Example

```
send-icmp-fragmentation
```

Syntax

```
no send-icmp-fragmentation
```

Mode

Interface

Description

Suppress ICMP fragmentation needed message generation.

Example

```
no send-icmp-fragmentation
```

Syntax

```
fragment-packets
```

Mode

Interface

Tunnel Interface VPN

Description

Enable fragment non-VPN outbound packets larger than this interface's MTU.

Example

```
fragment-packets
```

Syntax

```
no fragment-packets
```

Mode

Interface

Tunnel Interface VPN

Description

Disable fragment non-VPN outbound packets larger than this interface's MTU.

Example

```
no fragment-packets
```

Syntax

```
ignore-df-bit
```

Mode

Interface

Tunnel Interface VPN

Description

Enable ignore don't fragment (DF) bit.

Example

```
ignore-df-bit
```

Syntax

```
no ignore-df-bit
```

Mode

Interface
Tunnel Interface VPN

Description

Disable ignore don't fragment (DF) bit.

Example

```
no ignore-df-bit
```

Syntax

```
mtu <UINT16>
```

Mode

Interface

Description

Set interface MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
mtu 1500
```

Syntax

```
https-redirect
```

Mode

Interface

Description

Enable redirection from HTTP to HTTPS.

Example

```
https-redirect
```

Syntax

```
no https-redirect
```

Mode

Interface

Description

Disable redirection from HTTP to HTTPS.

Example

```
no https-redirect
```

Syntax

```
management { http | https | ping | snmp | ssh }
```

Mode

Interface

Tunnel Interface VPN

Description

Enable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
management https
```

Syntax

```
no management { http | https | ping | snmp | ssh }
```

Mode

Interface

Tunnel Interface VPN

Description

Disable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

no management https

Syntax

user-login [http] [https]

Mode

Interface
Tunnel Interface VPN

Description

Enable user login for the specified protocols.

Options

http HTTP.
https HTTPS.

Example

user-login http

Syntax

no user-login [http] [https]

Mode

Interface
Tunnel Interface VPN

Description

Disable user login for the specified protocols.

Options

http HTTP.
https HTTPS.

Example

no user-login http

Syntax

mac { default | override <INTERFACE_MAC> }

Mode

Interface

Description

Set MAC address used for this interface.

Options

<i>default</i>	Factory configured MAC.
<i>override</i>	Override factory configured MAC.
<i><INTERFACE_MAC></i>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>

Example

mac override 00:17:C5:0F:73:F4

Syntax

auto-discovery

Mode

Interface

Description

Enable auto discovery for sonicwall switches on the interface.

Example

auto-discovery

Syntax

no auto-discovery

Mode

Interface

Description

Disable auto discovery for sonicwall switches on the interface.

Example

no auto-discovery

Syntax

flow-reporting

Mode

Interface
Tunnel Interface VPN

Description

Enable flow reporting on the interface.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Interface
Tunnel Interface VPN

Description

Disable flow reporting on the interface.

Example

no flow-reporting

Syntax

multicast

Mode

Interface
Tunnel Interface VPN

Description

Enable multicast support.

Example

multicast

Syntax

no multicast

Mode

Interface
Tunnel Interface VPN

Description

Disable multicast support.

Example

no multicast

Syntax

cos-8021p

Mode

Interface

Description

Enable 802.1p support.

Example

cos-8021p

Syntax

no cos-8021p

Mode

Interface

Description

Disable 802.1p support.

Example

no cos-8021p

Syntax

exclude-route

Mode

Interface

Description

Enable exclude from route advertisement (NSM, OSPF, BGP, RIP).

Example

exclude-route

Syntax

no exclude-route

Mode

Interface

Description

Disable exclude from route advertisement (NSM, OSPF, BGP, RIP).

Example

no exclude-route

Syntax

asymmetric-route

Mode

Interface
Tunnel Interface VPN

Description

Enable asymmetric route.

Example

asymmetric-route

Syntax

no asymmetric-route

Mode

Interface
Tunnel Interface VPN

Description

Disable asymmetric route.

Example

no asymmetric-route

Syntax

management-traffic-only

Mode

Interface

Description

Enable management traffic only.

Example

management-traffic-only

Syntax

no management-traffic-only

Mode

Interface

Description

Disable management traffic only.

Example

no management-traffic-only

Syntax

dns-proxy

Mode

Interface

Description

Enable DNS proxy on the interface.

Example

dns-proxy

Syntax

no dns-proxy

Mode

Interface

Description

Disable DNS proxy on the interface.

Example

no dns-proxy

Syntax

default-8021p-cos { background | best-effort | controlled-load | excellent-effort | network-control | spare | video | voice }

Mode

Interface

Description

Enable default 802.1p CoS.

Options

<i>background</i>	1-Background.
<i>best-effort</i>	0-Best effort.
<i>controlled-load</i>	4-Controlled load.
<i>excellent-effort</i>	3-Excellent effort.
<i>network-control</i>	7-Network control.
<i>spare</i>	2-Spare.
<i>video</i>	5-Video(<100ms latency).
<i>voice</i>	6-Voice(<10ms latency).

Example

default-8021p-cos best-effort

Syntax

no default-8021p-cos

Mode

Interface

Description

Disable default 802.1p CoS.

Example

no default-8021p-cos

Syntax

shutdown-port

Mode

Interface

Description

Enable shutdown port.

Example

shutdown-port

Syntax

no shutdown-port

Mode

Interface

Description

Disable shutdown port.

Example

```
no shutdown-port
```

Syntax

```
secondary ip <IPV4_HOST>
```

Mode

Interface

Description

Set secondary IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
secondary ip 2.2.2.2
```

Syntax

```
no secondary ip
```

Mode

Interface

Description

Clear secondary IP address.

Example

```
no secondary ip
```

Syntax

```
secondary netmask <IPV4_MASK>
```

Mode

Interface

Description

Set secondary subnet mask.

Options

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
secondary netmask 255.255.255.0
```

Syntax

no secondary netmask

Mode

Interface

Description

Clear secondary subnet mask.

Example

no secondary netmask

Syntax

port aggregation aggregate <UINT8> <PORT_GROUP_INTERFACE>

Mode

Interface

Description

Set link aggregation.

Options

<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><PORT_GROUP_INTERFACE></i>	Interface name. Example: <i>X0</i>

Example

port aggregation aggregate 1 X3
port aggregation aggregate 2 X4
port aggregation aggregate 3 X5

Syntax

no port aggregation aggregate <UINT8>

Mode

Interface

Description

Disable link aggregate port.

Options

<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

no port aggregation aggregate 1

Syntax

port aggregation paired-aggregate <UINT8> <PORT_GROUP_INTERFACE>

Mode

Interface

Description

Set paired interface link aggregation.

Options

- <UINT8>

Integer in the form: D OR 0xHH.
Example: 123
- <PORT_GROUP_INTERFACE>

Interface name.
Example: X0

Example

```
port aggregation paired-aggregate 1 X6
port aggregation paired-aggregate 2 X7
port aggregation paired-aggregate 3 X8
```

Syntax

```
no port aggregation paired-aggregate <UINT8>
```

Mode

Interface

Description

Disable paired interface link aggregate port.

Options

- <UINT8>

Integer in the form: D OR 0xHH.
Example: 123

Example

```
no port aggregation paired-aggregate 1
```

Syntax

```
port redundancy <PORT_GROUP_INTERFACE>
```

Mode

Interface

Description

Set port redundancy.

Options

- <PORT_GROUP_INTERFACE>

Interface name.
Example: X0

Example

```
port redundancy X3
```

Syntax

```
no port redundancy-aggregation
```

Mode

Interface

Description

Disable port redundancy and link aggregation.

Example

```
no port redundancy-aggregation
```

Syntax

```
load-balancing-vip <IPV4_HOST>
```

Mode

Interface

Description

Set the LAN load balancing virtual IP address for active-active cluster.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
load-balancing-vip 10.10.10.15
```

Syntax

```
no load-balancing-vip
```

Mode

Interface

Description

Remove the LAN load balancing virtual IP address for active-active cluster.

Example

```
no load-balancing-vip
```

Syntax

```
routed-mode { any | interface <PHYS_WAN_INTERFACE> }
```

Mode

Interface

Description

Enable routed mode and set the associated interface - Add NAT policy to prevent inbound / outbound translation.

Options

any Use any interface.

interface Specify interface.

<PHYS_WAN_INTERFACE> WAN interface name.
Example: *X1*

Example

```
routed-mode interface X1
```

Syntax

```
no routed-mode
```

Mode

Interface

Description

Disable routed mode.

Example

```
no routed-mode
```

Syntax

```
sonicpoint limit <SONICPOINT_LIMIT>
```

Mode

Interface

Description

Set SonicPoint limit.

Options

<SONICPOINT_LIMIT>	SonicPoint limit per interface. Example: 8

Example

```
sonicpoint limit 8
```

Syntax

```
no sonicpoint limit
```

Mode

Interface

Description

Set SonicPoint limit.

Example

```
no sonicpoint limit
```

Syntax

```
sonicpoint reserve-address { dynamic | manual <IPV4_HOST> }
```

Mode

Interface

Description

Set dynamically or manually reserve SonicPoint address.

Options

<i>dynamic</i>	Dynamically reserve SonicPoint address.
<i>manual</i>	Manually reserve SonicPoint address.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
sonicpoint reserve-address dynamic
```

Syntax

```
ip-assignment <INTERFACE_ZONE_NAME> [ mode ] { dhcp | l2bridge | l2tp | portshield <PORTSHIELD_TO_INTERFACE> | ppoe | pptp | static | tap-mode | transparent | unnumbered | wire-mode }
```

Mode

Interface
Tunnel Interface VPN

Description

Set interface zone and IP assignment.

Options

<i><INTERFACE_ZONE_NAME></i>	Zone object name. Example: <i>DMZ</i>
<i>mode</i>	Interface IP assignment mode.
<i>dhcp</i>	IP address obtained by DHCP.
<i>l2bridge</i>	Interface uses layer two bridging (IP route option).
<i>l2tp</i>	Interface uses layer2 tunneling protocol.
<i>portshield</i>	Interface is portshielded.
<i><PORTSHIELD_TO_INTERFACE></i>	Interface name. Example: <i>X0</i>
<i>ppoe</i>	Interface uses point to point protocol over ethernet.
<i>pptp</i>	Interface uses point to point tunneling protocol.
<i>static</i>	Static IP address assignment.
<i>tap-mode</i>	Interface in tap mode.
<i>transparent</i>	Interface uses transparent bridging (splice L3 subnet).
<i>unnumbered</i>	Unnumbered IP address assignment.
<i>wire-mode</i>	Interfaces paired in wire mode.

Example

```
ip-assignment WAN dhcp
ip-assignment WLAN static
ip-assignment LAN l2bridge
ip-assignment MGMT static
ip-assignment LAN wire-mode
```

Syntax

```
no ip-assignment
```

Mode

Interface

Description

Clear interface zone and IP assignment.

Example

```
no ip-assignment
```

Syntax

```
native-bridge <NATIVE_BRIDGE_INTERFACE>
```

Mode

Interface

Description

Configure this interface to native bridge mode and set the interface to which native bridge to.

Options

<NATIVE_BRIDGE_INTERFACE> Interface name.
Example: *X0*

Example

```
native-bridge X0
```

Syntax

```
no native-bridge
```

Mode

Interface

Description

Disable native bridge mode.

Example

```
no native-bridge
```

Syntax

```
firewalling
```

Mode

Interface

Description

Enable firewalling with other bridge members.

Example

```
firewalling
```

Syntax

```
no firewalling
```

Mode

Interface

Description

Disable firewalling with other bridge members.

Example

```
no firewalling
```

Syntax

```
type { bypass | inspect | secure }
```

Mode

Wire Mode

Description

Set the type for wiremode.

Options

bypass Bypass (via internal switch / relay).

inspect Inspect (passive deep packet inspection of mirrored traffic).

secure Secure (active deep packet inspection of inline traffic).

Example

```
type secure
```

Syntax

```
paired-interface <PORT_GROUP_INTERFACE>
```

Mode

Wire Mode

Description

Set the paired interface for wiremode.

Options

<PORT_GROUP_INTERFACE> Interface name.
Example: *X0*

Example

```
paired-interface X3
```

Syntax

```
no paired-interface
```

Mode

Wire Mode

Description

Clear the paired interface for wiremode.

Example

```
no paired-interface
```

Syntax

```
paired-interface-zone <WIRE_INTERFACE_ZONE_NAME>
```

Mode

Wire Mode

Description

Set the paired interface zone for wiremode.

Options

<WIRE_INTERFACE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
paired-interface-zone LAN
```

Syntax

```
stateful-inspection
```

Mode

Wire Mode

Tap Mode

Description

Enable stateful inspection.

Example

```
stateful-inspection
```

Syntax

```
no stateful-inspection
```

Mode

Wire Mode

Tap Mode

Description

Disable stateful inspection.

Example

```
no stateful-inspection
```

Syntax

```
linkstate-propagation
```

Mode

Wire Mode

Description

Enable link state propagation.

Example

```
linkstate-propagation
```

Syntax

```
no linkstate-propagation
```

Mode

Wire Mode

Description

Disable link state propagation.

Example

```
no linkstate-propagation
```

Syntax

```
restrict-analysis
```

Mode

Wire Mode

Description

Enable restrict analysis at resource limit.

Example

```
restrict-analysis
```

Syntax

```
no restrict-analysis
```

Mode

Wire Mode

Description

Disable restrict analysis at resource limit.

Example

```
no restrict-analysis
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

Static IP Assignment

Description

Set interface IP address.

Options

- <IPV4_HOST>** IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- netmask** Set interface netmask.
- <IPV4_MASK>** IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

Static IP Assignment

Description

Clear interface IP address.

Example

```
no ip
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Static IP Assignment

Description

Set interface subnet mask.

Options

- <IPV4_MASK>** IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
netmask 255.255.255.0
```

Syntax

```
no netmask
```

Mode

Static IP Assignment

Description

Clear interface subnet mask.

Example

```
no netmask
```

Syntax

```
dns primary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the primary DNS server IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
dns primary 192.168.168.169
```

Syntax

```
dns secondary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the secondary DNS server IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
dns secondary 192.168.168.170
```

Syntax

```
dns tertiary <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set the tertiary DNS server IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
dns tertiary 192.168.168.171
```

Syntax

```
no dns primary
```

Mode

Static IP Assignment

Description

Clear the primary DNS server IP address.

Example

```
no dns primary
```

Syntax

```
no dns secondary
```

Mode

Static IP Assignment

Description

Clear the secondary DNS server IP address.

Example

```
no dns secondary
```

Syntax

```
no dns tertiary
```

Mode

Static IP Assignment

Description

Clear the tertiary DNS server IP address.

Example

```
no dns tertiary
```

Syntax

```
one-arm-mode
```

Mode

Interface

Description

Enable interface one-arm mode.

Example

```
one-arm-mode
```

Syntax

```
no one-arm-mode
```

Mode

Interface

Description

Disable interface one-arm mode.

Example

```
no one-arm-mode
```

Syntax

```
one-arm-peer <IPV4_HOST>
```

Mode

Interface

Description

Set interface one-arm peer.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
one-arm-peer 10.10.10.1
```

Syntax

```
no one-arm-peer
```

Mode

Interface

Description

Disable interface one-arm peer.

Example

```
no one-arm-peer
```

Syntax

```
gateway <IPV4_HOST>
```

Mode

Static IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
gateway 10.10.10.1
```

Syntax

no gateway

Mode

Static IP Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

hostname <WORD>

Mode

DHCP IP Assignment

Description

Set DHCP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

hostname mydhcpclient

Syntax

no hostname

Mode

DHCP IP Assignment

Description

Clear DHCP hostname.

Example

no hostname

Syntax

release

Mode

DHCP IP Assignment

Description

Release designated interface DHCP lease.

Example

release

Syntax

renew

Mode

DHCP IP Assignment

Description

Renew interface DHCP lease.

Example

renew

Syntax

renew-on-startup

Mode

DHCP IP Assignment

Description

Enable request renew of previous IP on startup.

Example

renew-on-startup

Syntax

no renew-on-startup

Mode

DHCP IP Assignment

Description

Disable request renew of previous IP on startup.

Example

no renew-on-startup

Syntax

renew-on-link-up

Mode

DHCP IP Assignment

Description

Enable renew DHCP lease on any link up occurrence.

Example

renew-on-link-up

Syntax

no renew-on-link-up

Mode

DHCP IP Assignment

Description

Disable renew DHCP lease on any link up occurrence.

Example

```
no renew-on-link-up
```

Syntax

```
initiate-renewals-with-discover
```

Mode

DHCP IP Assignment

Description

Enable initiate renewals with a discover when using DHCP.

Example

```
initiate-renewals-with-discover
```

Syntax

```
no initiate-renewals-with-discover
```

Mode

DHCP IP Assignment

Description

Disable initiate renewals with a discover when using DHCP.

Example

```
no initiate-renewals-with-discover
```

Syntax

```
force-discover-interval <UINT32>
```

Mode

DHCP IP Assignment

Description

Enable and set the DHCP discovers interval during lease acquisition.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
force-discover-interval 8
```

Syntax

no force-discover-interval

Mode

DHCP IP Assignment

Description

Disable force DHCP discovers interval during lease acquisition.

Example

no force-discover-interval

Syntax

schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

PPTP IP Assignment

Description

Set the wan pptp reconnect schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "Work Hours"

Syntax

dynamic

Mode

PPTP IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

dynamic

Syntax

no dynamic

Mode

PPTP IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

```
no dynamic
```

Syntax

```
gateway <IPV4_HOST>
```

Mode

PPTP IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
gateway 10.10.10.1
```

Syntax

```
no gateway
```

Mode

PPTP IP Assignment

Description

Clear interface gateway.

Example

```
no gateway
```

Syntax

```
hostname <WORD>
```

Mode

PPTP IP Assignment

Description

Set PPTP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
hostname mypptpclient
```

Syntax

no hostname

Mode

PPTP IP Assignment

Description

Clear PPTP hostname.

Example

no hostname

Syntax

inactivity <UINT16>

Mode

PPTP IP Assignment

Description

Enable the PPTP inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

inactivity 10

Syntax

no inactivity

Mode

PPTP IP Assignment

Description

Disable the PPTP inactivity timer.

Example

no inactivity

Syntax

ip <IPV4_HOST> [netmask <IPV4_MASK>]

Mode

PPTP IP Assignment

Description

Set PPTP IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

netmask Set interface netmask.

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

PPTP IP Assignment

Description

Clear PPTP IP address.

Example

```
no ip
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

PPTP IP Assignment

Description

Set PPTP user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

```
no password
```

Mode

PPTP IP Assignment

Description

Clear PPTP user password.

Example

```
no password
```

Syntax

```
release
```

Mode

PPTP IP Assignment

Description

Release designated interface DHCP lease.

Example

```
release
```

Syntax

```
renew
```

Mode

PPTP IP Assignment

Description

Renew interface DHCP lease.

Example

```
renew
```

Syntax

```
server <IPV4_HOST>
```

Mode

PPTP IP Assignment

Description

Set PPTP server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
server 10.10.10.10
```

Syntax

```
no server
```

Mode

PPTP IP Assignment

Description

Clear PPTP server IP address.

Example

```
no server
```

Syntax

user-name <WORD>

Mode

PPTP IP Assignment

Description

Set PPTP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name pptpuser

Syntax

no user-name

Mode

PPTP IP Assignment

Description

Clear PPTP user name.

Example

no user-name

Syntax

schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

L2TP IP Assignment

Description

Set the wan l2tp reconnect schedule.

Options

- always-on*** Always on.
- days*** Schedule object days.
<SCHED_DAYS> Days of the week in the form: SU-M-T-W-TH-F-SA.
Example: *SU-M-TH-SA*
- time*** Schedule object beginning/ending time.
<SCHED_TIME_BEGIN> Time in the form: DD:DD.
Example: *12:00*
<SCHED_TIME_END> Time in the form: DD:DD.
Example: *12:00*
- name*** Schedule object name.
<SCHED_NAME> Schedule object name.
Example: *Work Hours*

Example

schedule name "Work Hours"

Syntax

dynamic

Mode

L2TP IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

dynamic

Syntax

no dynamic

Mode

L2TP IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

no dynamic

Syntax

gateway <IPV4_HOST>

Mode

L2TP IP Assignment

Description

Set interface gateway.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

gateway 10.10.10.1

Syntax

no gateway

Mode

L2TP IP Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

hostname <WORD>

Mode

L2TP IP Assignment

Description

Set L2TP hostname.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

hostname myl2tpclient

Syntax

no hostname

Mode

L2TP IP Assignment

Description

Clear L2TP hostname.

Example

no hostname

Syntax

inactivity <UINT16>

Mode

L2TP IP Assignment

Description

Enable the L2TP inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

inactivity 10

Syntax

no inactivity

Mode

L2TP IP Assignment

Description

Disable the L2TP inactivity timer.

Example

```
no inactivity
```

Syntax

```
ip <IPV4_HOST> [ netmask <IPV4_MASK> ]
```

Mode

L2TP IP Assignment

Description

Set L2TP IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

netmask Set interface netmask.

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
ip 10.10.10.10 netmask 255.255.255.0
```

Syntax

```
no ip
```

Mode

L2TP IP Assignment

Description

Clear L2TP IP address.

Example

```
no ip
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

L2TP IP Assignment

Description

Set L2TP user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

no password

Mode

L2TP IP Assignment

Description

Clear L2TP password.

Example

no password

Syntax

release

Mode

L2TP IP Assignment

Description

Release designated interface DHCP lease.

Example

release

Syntax

renew

Mode

L2TP IP Assignment

Description

Renew interface DHCP lease.

Example

renew

Syntax

server <IPv4_HOST>

Mode

L2TP IP Assignment

Description

Set L2TP server IP address.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

server 10.10.10.10

Syntax

no server

Mode

L2TP IP Assignment

Description

Clear L2TP server IP address.

Example

no server

Syntax

shared-secret <ENC_PASSWORD>

Mode

L2TP IP Assignment

Description

Set L2TP password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

shared-secret myl2tpsecret

Syntax

no shared-secret

Mode

L2TP IP Assignment

Description

Clear L2TP shared secret.

Example

no shared-secret

Syntax

user-name <WORD>

Mode

L2TP IP Assignment

Description

Set L2TP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name l2tpuser
```

Syntax

```
no user-name
```

Mode

L2TP IP Assignment

Description

Clear L2TP user name.

Example

```
no user-name
```

Syntax

```
dynamic
```

Mode

PPPoE IP Assignment

Description

Enable dynamic acquisition of IP configuration data.

Example

```
dynamic
```

Syntax

```
no dynamic
```

Mode

PPPoE IP Assignment

Description

Disable dynamic acquisition of IP configuration data.

Example

```
no dynamic
```

Syntax

```
unnumbered <UNNUMBERED_INTERFACE_NAME>
```

Mode

PPPoE IP Assignment

Description

Set unnumbered interface.

Options

<UNNUMBERED_INTERFACE_NAME> Interface name.

Example

```
unnumbered X3
```

Syntax

```
no unnumbered
```

Mode

PPPoE IP Assignment

Description

Clear unnumbered interface.

Example

```
no unnumbered
```

Syntax

```
inactivity <UINT16>
```

Mode

PPPoE IP Assignment

Description

Enable the PPPoE inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
inactivity 10
```

Syntax

```
no inactivity
```

Mode

PPPoE IP Assignment

Description

Disable the PPPoE inactivity timer.

Example

```
no inactivity
```

Syntax

```
ip <IPv4_HOST>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ip 10.10.10.10
```

Syntax

```
no ip
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE IP address.

Example

```
no ip
```

Syntax

```
lcp-echo-packets
```

Mode

PPPoE IP Assignment

Description

Enable strictly use LCP echo packets for server keep-alive.

Example

```
lcp-echo-packets
```

Syntax

```
no lcp-echo-packets
```

Mode

PPPoE IP Assignment

Description

Disable strictly use LCP echo packets for server keep-alive.

Example

```
no lcp-echo-packets
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mysecret
```

Syntax

```
no password
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE password.

Example

```
no password
```

Syntax

```
service-name <WORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE service Name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
service-name mypppoeservice
```

Syntax

```
no service-name
```

Mode

PPPoE IP Assignment

Description

Clear PPPoE service Name.

Example

```
no service-name
```

Syntax

```
reconnect <UINT16>
```

Mode

PPPoE IP Assignment

Description

Enable and set reconnect the PPPoE client if the server does not send traffic for specified minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
reconnect 5
```

Syntax

```
ncp_neg_retrans <UINT16>
```

Mode

PPPoE IP Assignment

Description

Set the NCP retransmission time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
ncp_neg_retrans 200
```

Syntax

```
no reconnect
```

Mode

PPPoE IP Assignment

Description

Disable reconnect the PPPoE client if the server does not send traffic.

Example

```
no reconnect
```

Syntax

```
user-name <WORD>
```

Mode

PPPoE IP Assignment

Description

Set PPPoE user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name pppoeuser

Syntax

no user-name

Mode

PPPoE IP Assignment

Description

Clear PPPoE user name.

Example

no user-name

Syntax

schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

PPPoE IP Assignment

Description

Set the wan pppoe reconnect schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "Work Hours"

Syntax

bridge-to <L2BRIDGE_INTERFACE>

Mode

L2 Bridge

Description

Configure interface to which this interface is bridged to.

Options

<L2BRIDGE_INTERFACE> Interface name.
Example: *X0*

Example

bridge-to X1

Syntax

block-non-ip

Mode

L2 Bridge

Description

Enable block all non-IP traffic.

Example

block-non-ip

Syntax

no block-non-ip

Mode

L2 Bridge

Description

Disable block all non-IP traffic.

Example

no block-non-ip

Syntax

route-on-bridge-pair

Mode

L2 Bridge

Description

Route traffic on this bridge-pair.

Example

route-on-bridge-pair

Syntax

no route-on-bridge-pair

Mode

L2 Bridge

Description

Never route traffic on this bridge-pair.

Example

```
no route-on-bridge-pair
```

Syntax

```
only-sniff
```

Mode

L2 Bridge

Description

Enable only sniff traffic on this bridge-pair.

Example

```
only-sniff
```

Syntax

```
no only-sniff
```

Mode

L2 Bridge

Description

Disable only sniff traffic on this bridge-pair.

Example

```
no only-sniff
```

Syntax

```
stateful-inspection
```

Mode

L2 Bridge

Description

Enable stateful-inspection on this bridge-pair.

Example

```
stateful-inspection
```

Syntax

```
no stateful-inspection
```

Mode

L2 Bridge

Description

Disable stateful-inspection on this bridge-pair.

Example

```
no stateful-inspection
```

Syntax

```
vlan-filtering-mode { allow | block }
```

Mode

L2 Bridge

Description

Set VLAN filtering Mode.

Options

allow Allow.

block Block.

Example

```
vlan-filtering-mode block
```

Syntax

```
filtered-vlan <VLAN_FILTER_TAG>
```

Mode

L2 Bridge

Description

Add specified VLAN to filter.

Options

<VLAN_FILTER_TAG> Filtered VLAN ID list.
Example: 23

Example

```
filtered-vlan 100
```

Syntax

```
no filtered-vlan <VLAN_FILTER_TAG>
```

Mode

L2 Bridge

Description

Remove specified VLAN from filter.

Options

<VLAN_FILTER_TAG> Filtered VLAN ID list.
Example: 23

Example

```
no filtered-vlan 100
```

Syntax

no filtered-vlans

Mode

L2 Bridge

Description

Remove all filtered VLANs.

Example

no filtered-vlans

Syntax

no transparent-range

Mode

Transparent

Description

Clear the WAN addresses that are connected to this interface.

Example

no transparent-range

Syntax

transparent-range { group <WAN_ADDR_GROUP_NAME> | host <WAN_ADDR_HOST> | name <WAN_ADDR_HOST_NETWORK_RANGE_NAME> | network <WAN_ADDR_NETWORK> <ADDR_MASK> | range <WAN_ADDR_BEGIN> <ADDR_END> }

Mode

Transparent

Description

Set the WAN addresses that are connected to this interface.

Options

group <WAN_ADDR_GROUP_NAME>	Set transparent addresses to named address group. WAN group address object name. Example: <i>Sales Group</i>
host <WAN_ADDR_HOST>	Set transparent address as host address. WAN address object IPv4 host address in the form: D.D.D.D. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name <WAN_ADDR_HOST_NETWORK_RANGE_NAME>	Set transparent addresses to named address object. WAN address object name. Example: <i>X1 IP</i>
network <WAN_ADDR_NETWORK> <ADDR_MASK>	Set transparent addresses to network address. WAN address object IPv4 network in the form: D.D.D.D. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Set transparent addresses to range of addresses.

<WAN_ADDR_BEGIN>	WAN address object IPv4 starting range in the form: D.D.D.D. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:3257:ef fe\n</i>

Example

transparent-range name "WAN Transparent Range"

Syntax

gratuitous-arp-wan-forwarding

Mode

Transparent

Description

Enable gratuitous ARP forwarding towards WAN.

Example

gratuitous-arp-wan-forwarding

Syntax

no gratuitous-arp-wan-forwarding

Mode

Transparent

Description

Disable gratuitous ARP forwarding towards WAN.

Example

no gratuitous-arp-wan-forwarding

Syntax

gratuitous-arp-wan-generation

Mode

Transparent

Description

Enable automatic gratuitous ARP generation towards WAN.

Example

gratuitous-arp-wan-generation

Syntax

no gratuitous-arp-wan-generation

Mode

Transparent

Description

Disable automatic gratuitous ARP generation towards WAN.

Example

```
no gratuitous-arp-wan-generation
```

Syntax

```
arp
```

Mode

Config

Description

Enter ARP configuration mode.

Example

```
arp
```

Syntax

```
no entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE>
```

Mode

ARP

Description

Deletes an ARP entry.

Options

<ARP_IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<ARP_MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
<ARP_INTERFACE>	Interface name. Example: <i>X0</i>

Example

```
no entry 10.10.10.10 00:01:02:03:04:05 X0
```

Syntax

```
no entries
```

Mode

ARP

Description

Deletes all ARP entries.

Example

```
no entries
```

Syntax

```
entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE>
```

Mode

ARP

Description

Add/edit an ARP entry.

Options

- <ARP_IPV4_HOST>** IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- <ARP_MAC>** MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*
- <ARP_INTERFACE>** Interface name.
Example: *X0*

Example

entry 10.10.10.10 00:01:02:03:04:05 X0

Syntax

timeout <UINT16>

Mode

ARP

Description

Set the ARP cache entry timeout in minutes.

Options

- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

timeout 10

Syntax

glean

Mode

ARP

Description

Enable glean source data from ARP requests.

Example

glean

Syntax

no glean

Mode

ARP

Description

Disable glean source data from ARP requests.

Example

```
no glean
```

Syntax

```
ip <ARP_IPV4_HOST>
```

Mode

Static ARP

Description

Configure static ARP IP.

Options

<ARP_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ip 10.10.10.10
```

Syntax

```
mac <ARP_MAC>
```

Mode

Static ARP

Description

Configure static ARP MAC address.

Options

<ARP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
mac 00:01:02:03:04:05
```

Syntax

```
interface <ARP_INTERFACE>
```

Mode

Static ARP

Description

Configure static ARP interface.

Options

<ARP_INTERFACE> Interface name.
Example: *X0*

Example

```
interface X0
```

Syntax

publish

Mode

Static ARP

Description

Publish ARP entry.

Example

publish

Syntax

no publish

Mode

Static ARP

Description

Disable publishing of ARP entry.

Example

no publish

Syntax

bind-mac

Mode

Static ARP

Description

Enable MAC binding.

Example

bind-mac

Syntax

no bind-mac

Mode

Static ARP

Description

Disable MAC binding.

Example

no bind-mac

Syntax

dynamic

Mode

Static ARP

Description

Enable update IP address dynamically.

Example

dynamic

Syntax

no dynamic

Mode

Static ARP

Description

Disable update IP address dynamically.

Example

no dynamic

Syntax

clear arp cache entries

Mode

Config
ARP
Top Level

Description

Clear all non-permanent entries.

Example

clear arp cache entries

Syntax

clear arp cache entry <ARP_FLUSH_IPV4_HOST> <ARP_FLUSH_INTERFACE>

Mode

Config
ARP
Top Level

Description

Clear an ARP entry.

Options

- <ARP_FLUSH_IPV4_HOST>** IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- <ARP_FLUSH_INTERFACE>** Interface name.
Example: *X0*

Example

clear arp cache entry 10.10.10.10 X0

Syntax

```
dns server { inherit | ipv6 { inherit | preferred | static { primary <HOST_IP> | secondary <HOST_IP> | tertiary <HOST_IP> } } | static { primary <HOST_IP> | secondary <HOST_IP> | tertiary <HOST_IP> } }
```

Mode

Config

Description

Set DNS server.

Options

inherit	Inherit DNS servers.
ipv6	Set IPv6 DNS server
inherit	Inherit DNS servers.
preferred	Prefer IPv6 DNS Servers.
static	Set static DNS server
primary	Specify primary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
secondary	Specify secondary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
tertiary	Specify tertiary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
static	Set static DNS server
primary	Specify primary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
secondary	Specify secondary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
tertiary	Specify tertiary DNS server IP address.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

```
dns server static primary 192.168.168.165
dns server static secondary 192.168.168.165
dns server static tertiary 192.168.168.165
dns server inherit
dns server ipv6 static preferred
dns server ipv6 static primary fe80::0001
dns server ipv6 static secondary fe80::0001
dns server ipv6 static tertiary fe80::0001
dns server ipv6 inherit
```

Syntax

```
no dns server { inherit | ipv6 { inherit | preferred | static { primary | secondary | tertiary } } | static { primary | secondary | tertiary } }
```

Mode

Config

Description

Clear DNS server.

Options

<i>inherit</i>	Inherit DNS servers.
<i>ipv6</i>	Clear IPv6 DNS server
<i>inherit</i>	Inherit DNS servers.
<i>preferred</i>	Do not prefer IPv6 DNS Servers.
<i>static</i>	Clear static DNS server
<i>primary</i>	Clear primary DNS server IP address.
<i>secondary</i>	Clear secondary DNS server IP address.
<i>tertiary</i>	Clear tertiary DNS server IP address.
<i>static</i>	Clear static DNS server
<i>primary</i>	Clear primary DNS server IP address.
<i>secondary</i>	Clear secondary DNS server IP address.
<i>tertiary</i>	Clear tertiary DNS server IP address.

Example

```
no dns server static primary
no dns server static secondary
no dns server static tertiary
no dns server ipv6 preferred
no dns server ipv6 static primary
no dns server ipv6 static secondary
no dns server ipv6 static tertiary
```

Syntax

```
dns rebinding { action { drop-dns-reply | log-attack-only | return-query-refused } | allowed-domains { fqdn <ADDR_FQDN> |
group <ADDR_CUSTOM_FQDN_GROUP_NAME_MIXED> | name <ADDR_FQDN_NAME> } | enable }
```

Mode

Config

Description

Enable and configure DNS rebinding attack prevention.

Options

<i>action</i>	Set action when experiencing attack.
<i>drop-dns-reply</i>	Log the attack and drop the DNS reply.
<i>log-attack-only</i>	Log the attack only.
<i>return-query-refused</i>	Log the attack and return a query refused reply.
<i>allowed-domains</i>	Specify the domains for which checking is not done.

<i>fqdn</i>	Create FQDN address object with same name as defined.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i>	Specify FQDN group name.
<ADDR_CUSTOM_FQDN_GROUP_NAME_MIXED>	FQDN custom group address object name. Example: <i>Sales Group</i>
<i>name</i>	Specify FQDN address object name.
<ADDR_FQDN_NAME>	FQDN address object name. Example: <i>www.example.com</i>
<i>enable</i>	Enable DNS rebinding attack prevention.

Example

```
dns rebinding enable
dns rebinding action drop-dns-reply
dns rebinding allowed-domains name "DNS RAP WHITELIST"
```

Syntax

```
no dns rebinding { allowed-domains | enable }
```

Mode

Config

Description

Disable DNS rebinding attack prevention.

Options

- allowed-domains*** Clear DNS rebinding allowed domains.
- enable*** Disable DNS rebinding attack prevention.

Example

```
no dns rebinding enable
no dns rebinding allowed-domains
```

Syntax

```
dns fqdn-binding
```

Mode

Config

Description

Enable FQDN object only cache DNS reply from sanctioned server.

Example

```
dns fqdn-binding
```

Syntax

```
no dns fqdn-binding
```

Mode

Config

Description

Disable FQDN object only cache DNS reply from sanctioned server.

Example

```
no dns fqdn-binding
```

Syntax

```
dns split-servers
```

Mode

Config

Description

Enable proxying of split DNS servers.

Example

```
dns split-servers
```

Syntax

```
no dns split-servers
```

Mode

Config

Description

Disable proxying of split DNS servers.

Example

```
no dns split-servers
```

Syntax

```
no dns split-entries
```

Mode

Config

Description

Delete all the split DNS entries.

Example

```
no dns split-entries
```

Syntax

```
no dns split-entry <DNS_SPLIT_DNS_ENTRY_NAME>
```

Mode

Config

Description

Delete the specified split DNS entry.

Options

<DNS_SPLIT_DNS_ENTRY_NAME> Split DNS entry domain name.
Example: *sonicwall.com*

Example

```
no split-entry sonicwa.com
```

Syntax

```
dns split-entry <DNS_SPLIT_DNS_ENTRY_NAME>
```

Mode

Config

Description

Add/edit a split DNS entry and enter to its configuration mode.

Options

<DNS_SPLIT_DNS_ENTRY_NAME> Split DNS entry domain name.
Example: *sonicwall.com*

Example

```
split-entry sonicwall.com
```

Syntax

```
domain <DNS_SPLIT_DNS_ENTRY_NAME>
```

Mode

DNS split DNS entry.

Description

Set the split DNS entry domain name.

Options

<DNS_SPLIT_DNS_ENTRY_NAME> Split DNS entry domain name.
Example: *sonicwall.com*

Example

```
domain sonicwall.com
```

Syntax

```
no server ipv4 { primary | secondary | tertiary }
```

Mode

DNS split DNS entry.

Description

Clear the split DNS entry IPv4 server.

Options

primary Primary server.

secondary Secondary server.

tertiary Tertiary server.

Example

```
no server ipv4 primary
no server ipv4 secondary
no server ipv4 tertiary
```

Syntax

```
server ipv4 { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> }
```

Mode

DNS split DNS entry.

Description

Set the split DNS entry IPv4 server.

Options

primary Primary server.
<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Secondary server.
<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

tertiary Tertiary server.
<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
server ipv4 primary 10.10.10.10
server ipv4 secondary 10.10.10.10
server ipv4 tertiary 10.10.10.10
```

Syntax

```
no server ipv6 { primary | secondary | tertiary }
```

Mode

DNS split DNS entry.

Description

Clear the split DNS entry IPv6 server.

Options

primary Primary server.

secondary Secondary server.

tertiary Tertiary server.

Example

```
no server ipv6 primary
no server ipv6 secondary
no server ipv6 tertiary
```

Syntax

```
server ipv6 { primary <IPv6_HOST> | secondary <IPv6_HOST> | tertiary <IPv6_HOST> }
```

Mode

DNS split DNS entry.

Description

Set the split DNS entry IPv6 server.

Options

primary	Primary server.
<IPv6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
secondary	Secondary server.
<IPv6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
tertiary	Tertiary server.
<IPv6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
server ipv6 primary 2016::2016
server ipv6 secondary 2016::2016
server ipv6 tertiary 2016::2016
```

Syntax

```
no local-interface
```

Mode

DNS split DNS entry.

Description

Clear the local interface for split DNS entry.

Example

```
no local-interface
```

Syntax

```
local-interface <DNS_SPLIT_DNS_ENTRY_INTERFACE>
```

Mode

DNS split DNS entry.

Description

Set the local interface for split DNS entry.

Options

<DNS_SPLIT_DNS_ENTRY_INTERFACE>	Split DNS entry local interface name. Example: <i>X1</i>

Example

```
local-interface X1
```

Syntax

```
no manual-ttl
```

Mode

DNS split DNS entry.

Description

Disable manually set TTL value in DNS reply.

Example

```
no manual-ttl
```

Syntax

```
manual-ttl <UINT32>
```

Mode

DNS split DNS entry.

Description

Enable manually set TTL value in DNS reply and set TTL value(seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
manual-ttl 20
```

Syntax

```
dns fqdn-over-tcp-dns
```

Mode

Config

Description

Enable DNS host name lookup over TCP for FQDN.

Example

```
dns fqdn-over-tcp-dns
```

Syntax

```
no dns fqdn-over-tcp-dns
```

Mode

Config

Description

Disable DNS host name lookup over TCP for FQDN.

Example

```
no dns fqdn-over-tcp-dns
```

Syntax

```
clear dns cache [ interface-reverse ]
```

Mode

Config
Top Level

Description

Clear DNS cache.

Options

interface-reverse Clear interface names reverse DNS cache.

Example

```
clear dns cache
```

Syntax

```
no dynamic-dns profile [ ipv6 ] <DDNS_PROFILE_NAME>
```

Mode

Config

Description

Deletes a dynamic DNS profile.

Options

ipv6 Delete IPv6 dynamic DNS Profile.
<DDNS_PROFILE_NAME> Dynamic DNS profile name.
Example: *mydns*

Example

```
no dynamic-dns profile "abc"  
no dynamic-dns profile ipv6 "xyz"
```

Syntax

```
no dynamic-dns profiles [ ipv6 ]
```

Mode

Config

Description

Deletes all dynamic DNS profiles.

Options

ipv6 Delete all IPv6 dynamic DNS Profiles.

Example

```
no dynamic-dns profiles  
no dynamic-dns profiles ipv6
```

Syntax

```
dynamic-dns profile [ ipv6 ] <DDNS_PROFILE_NAME>
```

Mode

Config

Description

Add/edit a dynamic DNS profile.

Options

- ipv6** Add/edit an IPv6 dynamic DNS Profile.
- <DDNS_PROFILE_NAME>** Dynamic DNS profile name.
Example: *mydns*

Example

```
dynamic-dns profile CorpNoIP
dynamic-dns profile ipv6 CorpNoIP
```

Syntax

```
profile-name <DDNS_PROFILE_NAME>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Edit a dynamic DNS profile name.

Options

- <DDNS_PROFILE_NAME>** Dynamic DNS profile name.
Example: *mydns*

Example

```
profile-name CorpNoIP
```

Syntax

```
enable
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Enable dynamic DNS profile.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Disable dynamic DNS profile.

Example

```
no enable
```

Syntax

```
use-online
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Enable use online settings.

Example

```
use-online
```

Syntax

```
no use-online
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Disable use online settings.

Example

```
no use-online
```

Syntax

```
provider { changeip | dyn | noip }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Select dynamic DNS provider.

Options

changeip changeip.com.

dyn dyn.com.

noip No-IP.com.

Example

```
provider noip
```

Syntax

user-name <WORD>

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name ddnsadmin

Syntax

no user-name

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS user name.

Example

no user-name

Syntax

password <ENC_PASSWORD>

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password thisisasecret

Syntax

no password

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS password.

Example

```
no password
```

Syntax

```
domain <HOSTNAME>
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain testsite.hopto.org
```

Syntax

```
no domain
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Clear dynamic DNS domain.

Example

```
no domain
```

Syntax

```
bound-to { any | interface <WAN_INTERFACE> }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Set dynamic DNS WAN interface to bind to.

Options

any Any interface.

interface Specify interface.

<WAN_INTERFACE> WAN interface name.
Example: *X1*

Example

Syntax

```
online-settings { detect | manual <HOST_IP> | set-to-wan }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS online settings.

Options

detect	Let the dynamic DNS provider detect the IP address.
manual	Specify the IP address manually.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
set-to-wan	Automatically set the IP address to the primary WAN IP address.

Example

```
online-settings manual 10.10.10.10
```

Syntax

```
offline-settings { do-nothing | make-host-unknown | manual <IPV4_HOST> | use-previous }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS offline settings.

Options

do-nothing	Allows the previously registered IP address to remain current with the Provider.
make-host-unknown	Let the dynamic DNS provider detect the IP address.
manual	Specify the IP address manually.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
use-previous	Use the off-line IP address previously configured at the provider's site.

Example

```
offline-settings manual 10.10.10.10
```

Syntax

```
service-type { custom | dynamic | static }
```

Mode

Dynamic DNS
Dynamic IPv6 DNS

Description

Configure dynamic DNS service type.

Options

custom Custom.

dynamic Dynamic.

static Static.

Example

service-type dynamic

Syntax

dhcp-server [ipv4 | ipv6]

Mode

Config

Description

Enter DHCP server configuration mode.

Options

ipv4 Enter IPv4 DHCP server configuration mode.

ipv6 Enter IPv6 DHCP server configuration mode.

Example

dhcp-server

Syntax

enable

Mode

DHCP Server

Description

Enable DHCP server.

Example

enable

Syntax

no enable

Mode

DHCP Server

Description

Disable DHCP server.

Example

```
no enable
```

Syntax

```
conflict-detection
```

Mode

DHCP Server

Description

Enable DHCP server conflict detection.

Example

```
conflict-detection
```

Syntax

```
no conflict-detection
```

Mode

DHCP Server

Description

Disable DHCP server conflict detection.

Example

```
no conflict-detection
```

Syntax

```
persistence
```

Mode

DHCP Server

Description

Enable/configure DHCP server persistence.

Example

```
persistence
```

Syntax

```
no persistence
```

Mode

DHCP Server

Description

Disable DHCP server persistence.

Example

no persistence

Syntax

persistence-monitoring-interval <UINT16>

Mode

DHCP Server

Description

DHCP server persistence monitoring interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

persistence monitoring interval 5

Syntax

scope dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST>

Mode

DHCP Server

Description

Add/edit dynamic DHCP scope and enter its configuration mode.

Options

<SCOPE_START_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168
<SCOPE_END_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

scope dynamic 192.168.168.100 192.168.168.200

Syntax

no scope dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST>

Mode

DHCP Server

Description

Delete dynamic DHCP scope.

Options

<SCOPE_START_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168
<SCOPE_END_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

no scope dynamic 192.168.168.100 192.168.168.200

Syntax

scope static <STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC>

Mode

DHCP Server

Description

Add/edit static DHCP scope and enter its configuration mode.

Options

<STATIC_SCOPE_IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<STATIC_SCOPE_MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>

Example

scope static 192.168.168.101 00:01:02:03:04:05

Syntax

no scope static <STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC>

Mode

DHCP Server

Description

Delete static DHCP scope.

Options

<STATIC_SCOPE_IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<STATIC_SCOPE_MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>

Example

no scope static 192.168.168.101 00:01:02:03:04:05

Syntax

no scopes dynamic

Mode

DHCP Server

Description

Delete all dynamic DHCP scopes.

Example

no scopes dynamic

Syntax

no scopes static

Mode

DHCP Server

Description

Delete all static DHCP entries.

Example

```
no scopes static
```

Syntax

```
no scopes
```

Mode

DHCP Server

Description

Delete all DHCP server lease scopes.

Example

```
no scopes
```

Syntax

```
clear lease <DHCP_LEASE_IPV4_HOST>
```

Mode

DHCP Server

Description

Delete DHCP server lease.

Options

<DHCP_LEASE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
clear lease 1.1.1.1
```

Syntax

```
clear leases
```

Mode

DHCP Server

Description

Delete all DHCP server leases.

Example

```
clear leases
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

DHCP Server

Description

Add/edit DHCP server option object and enter its configuration mode.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

option object "LAN Specific DHCP Option"

Syntax

no option object <DHCP_OPTION_OBJECT>

Mode

DHCP Server

Description

Delete DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

no option object "LAN Specific DHCP Option"

Syntax

no option objects

Mode

DHCP Server

Description

Delete all DHCP server option objects.

Example

no option objects

Syntax

option group <DHCP_OPTION_GROUP>

Mode

DHCP Server

Description

Add/edit DHCP server option group and enter its configuration mode.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group "LAN Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP>
```

Mode

DHCP Server

Description

Delete DHCP server option group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
no option group "LAN Specific DHCP Options"
```

Syntax

```
no option groups
```

Mode

DHCP Server

Description

Delete all DHCP server option groups.

Example

```
no option groups
```

Syntax

```
trusted-relay-agents <ADDR_DHCP_TRUSTED_RELAY_AGENT_GROUP>
```

Mode

DHCP Server

Description

Enable and set trusted DHCP relay agent list.

Options

<ADDR_DHCP_TRUSTED_RELAY_AGENT_GROUP> Group address object name.
Example: *Default Trusted Relay Agent List*

Example

```
trusted-relay-agents "Trusted Relay Agents"
```

Syntax

```
no trusted-relay-agents
```

Mode

DHCP Server

Description

Disable trusted DHCP relay agent list.

Example

```
no trusted-relay-agents
```

Syntax

```
recycle-expired-lease <UINT8>
```

Mode

DHCP Server

Description

Enable aggressively and fully recycle expired DHCP leases in advance and set threshold in percent.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
recycle-expired-lease 30
```

Syntax

```
no recycle-expired-lease
```

Mode

DHCP Server

Description

Disable aggressively and fully recycle expired DHCP leases in advance.

Example

```
no recycle-expired-lease
```

Syntax

```
enable
```

Mode

Dynamic Scope

Description

Enable dynamic DHCP scope.

Example

```
enable
```

Syntax

no enable

Mode

Dynamic Scope

Description

Disable dynamic DHCP scope.

Example

no enable

Syntax

range <IPV4_HOST> <IPV4_HOST>

Mode

Dynamic Scope

Description

Set DHCP dynamic scope range.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

range 192.168.168.100 192.168.168.200

Syntax

lease-time <UINT16>

Mode

Dynamic Scope

Description

Set dynamic DHCP scope lease time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

lease-time 1440

Syntax

default-gateway <IPV4_HOST>

Mode

Dynamic Scope

Description

Set dynamic DHCP scope default gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
default-gateway 192.168.168.254
```

Syntax

```
no default-gateway
```

Mode

Dynamic Scope

Description

Clear dynamic DHCP scope default gateway.

Example

```
no default-gateway
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope subnet mask.

Options

<IPV4_MASK> IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: *255.255.255.0*

Example

```
netmask 255.255.255.0
```

Syntax

```
comment <WORD>
```

Mode

Dynamic Scope

Description

Set dynamic DHCP scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "my dynamic scope"
```

Syntax

no comment

Mode

Dynamic Scope

Description

Clear dynamic DHCP scope comment.

Example

no comment

Syntax

allow-bootp

Mode

Dynamic Scope

Description

Enable allow BOOTP clients to use range.

Example

allow-bootp

Syntax

no allow-bootp

Mode

Dynamic Scope

Description

Disable allow BOOTP clients to use range.

Example

no allow-bootp

Syntax

domain-name <HOSTNAME>

Mode

Dynamic Scope

Description

Set DHCP domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

domain-name example.com

Syntax

no domain-name

Mode

Dynamic Scope

Description

Clear DHCP domain name.

Example

no domain-name

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Dynamic Scope

Description

Manually set DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

<i>inherit</i>	Inherit DNS servers.
<i>static</i>	Static DNS server.
<i>primary</i> <i><IPV4_HOST></i>	Specify primary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>secondary</i> <i><IPV4_HOST></i>	Specify secondary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>tertiary</i> <i><IPV4_HOST></i>	Specify tertiary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
dns server static primary 192.168.168.165  
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

Dynamic Scope

Description

Manually clear DNS server IP address.

Options

<i>static</i>	Clear static DNS server IP address.
<i>primary</i>	Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

tertiary Clear tertiary DNS server IP address.

Example

```
no dns server static primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

Dynamic Scope

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Secondary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

Dynamic Scope

Description

Clear the WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
call-manager { primary <WORD> | secondary <WORD> | tertiary <WORD> }
```

Mode

Dynamic Scope

Description

Set VOIP call managers.

Options

primary Specify primary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

secondary Specify secondary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

tertiary Specify tertiary VOIP call manager address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
call-manager primary 192.168.168.161
```

Syntax

```
no call-manager { primary | secondary | tertiary }
```

Mode

Dynamic Scope

Description

Clear VOIP call managers.

Options

primary Clear primary VOIP call manager IP address.

secondary Clear secondary VOIP call manager IP address.

tertiary Clear tertiary VOIP call manager address.

Example

```
no call-manager primary
```

Syntax

```
network-boot { boot-file <WORD> | next-server <IPV4_HOST> | server-name <WORD> }
```

Mode

Dynamic Scope

Description

Set network boot parameters.

Options

boot-file Specify boot file.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

next-server Specify next server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

server-name Specify server name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
network-boot next-server 192.168.168.161
```

Syntax

```
no network-boot { boot-file | next-server | server-name }
```

Mode

Dynamic Scope

Description

Clear network boot parameters.

Options

boot-file Clear boot file.

next-server Clear next server.

server-name Clear server name.

Example

```
no network-boot next-server
```

Syntax

```
no generic-option
```

Mode

Dynamic Scope

Description

Clear DHCP generic option group.

Example

```
no generic-option
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

Dynamic Scope

Description

Set DHCP generic option group.

Options

group Specify generic option group.

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

<i>object</i>	Specify generic option object.
<i><DHCP_OPTION_OBJECT></i>	DHCP server option object name. Example: <i>Corp Network DHCP Options</i>

Example

generic-option object "NetServers"

Syntax

always-send-option

Mode

Dynamic Scope

Description

Enable send generic options always.

Example

always-send-option

Syntax

no always-send-option

Mode

Dynamic Scope

Description

Disable send generic options always.

Example

no always-send-option

Syntax

enable

Mode

Static Scope

Description

Enable static DHCP server scope.

Example

enable

Syntax

no enable

Mode

Static Scope

Description

Disable DHCP server scope.

Example

no enable

Syntax

name <WORD>

Mode

Static Scope

Description

Set DHCP static scope name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "My Domain Server"

Syntax

no name

Mode

Static Scope

Description

Clear DHCP static scope name.

Example

no name

Syntax

ip <STATIC_SCOPE_IPV4_HOST>

Mode

Static Scope

Description

Set DHCP static scope IP address.

Options

<STATIC_SCOPE_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

ip 10.10.10.10

Syntax

mac <STATIC_SCOPE_MAC>

Mode

Static Scope

Description

Set DHCP static scope ethernet address.

Options

<STATIC_SCOPE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
mac 00:01:02:03:04:05
```

Syntax

```
lease-time <UINT16>
```

Mode

Static Scope

Description

Set DHCP static scope lease time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
lease-time 1440
```

Syntax

```
default-gateway <IPV4_HOST>
```

Mode

Static Scope

Description

Set DHCP static scope default gateway.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
default-gateway 192.168.168.254
```

Syntax

```
no default-gateway
```

Mode

Static Scope

Description

Clear DHCP static scope default gateway.

Example

```
no default-gateway
```

Syntax

```
netmask <IPV4_MASK>
```

Mode

Static Scope

Description

Set DHCP static scope subnet mask.

Options

<IPV4_MASK> IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

```
netmask 255.255.255.0
```

Syntax

```
comment <WORD>
```

Mode

Static Scope

Description

Set DHCP static scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment "my static scope"
```

Syntax

```
no comment
```

Mode

Static Scope

Description

Clear DHCP static scope comment.

Example

```
no comment
```

Syntax

```
domain-name <HOSTNAME>
```

Mode

Static Scope

Description

Set DHCP domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain-name example.com
```

Syntax

```
no domain-name
```

Mode

Static Scope

Description

Clear DHCP domain name.

Example

```
no domain-name
```

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Static Scope

Description

Manually set DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

inherit Inherit DNS servers.

static Static DNS server.

primary Specify primary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Specify secondary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

tertiary Specify tertiary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
dns server inherit
dns server static primary 192.168.168.165
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

Static Scope

Description

Manually clear DNS server IP address.

Options

<i>static</i>	Static DNS server.
<i>primary</i>	Clear primary DNS server IP address.
<i>secondary</i>	Clear secondary DNS server IP address.
<i>tertiary</i>	Clear tertiary DNS server IP address.

Example

```
no dns server static primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

Static Scope

Description

Set the WINS server IP address.

Options

<i>primary</i>	Primary WINS server IP address.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>secondary</i>	Secondary WINS server IP address.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

Static Scope

Description

Clear the WINS server IP address.

Options

- primary** Primary WINS server IP address.
- secondary** Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
call-manager { primary <WORD> | secondary <WORD> | tertiary <WORD> }
```

Mode

Static Scope

Description

Set VOIP call managers.

Options

- primary** Specify primary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- secondary** Specify secondary VOIP call manager IP address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- tertiary** Specify tertiary VOIP call manager address.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
call-manager manual primary 192.168.168.161
```

Syntax

```
no call-manager { primary | secondary | tertiary }
```

Mode

Static Scope

Description

Clear VOIP call managers.

Options

- primary** Clear primary VOIP call manager IP address.
- secondary** Clear secondary VOIP call manager IP address.
- tertiary** Clear tertiary VOIP call manager address.

Example

```
no call-manager primary
```

Syntax

```
network-boot { boot-file <WORD> | next-server <IPV4_HOST> | server-name <WORD> }
```

Mode

Static Scope

Description

Set network boot parameters.

Options

- boot-file** Specify boot file.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- next-server** Specify next server.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- server-name** Specify server name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
network-boot next-server 192.168.168.161
```

Syntax

```
no network-boot { boot-file | next-server | server-name }
```

Mode

Static Scope

Description

Clear network boot parameters.

Options

- boot-file** Clear boot file.
- next-server** Clear next server.
- server-name** Clear server name.

Example

```
no network-boot next-server
```

Syntax

```
no generic-option
```

Mode

Static Scope

Description

Clear DHCP generic option group.

Example

```
no generic-option
```

Syntax

generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }

Mode

Static Scope

Description

Set DHCP generic option group.

Options

<i>group</i>	Specify generic option group.
<i><DHCP_OPTION_GROUP></i>	DHCP server option group name. Example: <i>Corp Network DHCP Group</i>
<i>object</i>	Specify generic option object.
<i><DHCP_OPTION_OBJECT></i>	DHCP server option object name. Example: <i>Corp Network DHCP Options</i>

Example

generic-option object "NetServers"

Syntax

always-send-option

Mode

Static Scope

Description

Enable send generic options always.

Example

always-send-option

Syntax

no always-send-option

Mode

Static Scope

Description

Disable send generic options always.

Example

no always-send-option

Syntax

name <DHCP_OPTION_OBJECT>

Mode

DHCP Option

Description

Set DHCP server option object name.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

name "LAN Specific DHCP Option"

Syntax

number <UINT8>

Mode

DHCP Option

Description

Set DHCP server option object number.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

number 53

Syntax

array

Mode

DHCP Option

Description

Enable DHCP server option array.

Example

array

Syntax

no array

Mode

DHCP Option

Description

Disable DHCP server option array.

Example

no array

Syntax

no value

Mode

DHCP Option

Description

Clear DHCP server option object value.

Example

no value

Syntax

no values

Mode

DHCP Option

Description

Clear all values of this DHCP server option object.

Example

no values

Syntax

value { boolean <UINT8> | domain-name <HOSTNAME> | four-byte <UINT32> | hex-string <HEX_STRING> | ip <IPV4_HOST> | one-byte <UINT8> | string <WORD> | two-byte <UINT16> }

Mode

DHCP Option

Description

Set DHCP server option object value.

Options

boolean <UINT8>	Option object type: boolean. Integer in the form: D OR 0xHH. Example: 123
domain-name <HOSTNAME>	Option object type: domain name. Hostname in the form: hostname OR a.b.c.d. Example: example.com
four-byte <UINT32>	Option object type: four byte. Integer in the form: D OR 0xHHHHHHHH. Example: 123
hex-string <HEX_STRING>	Option object type: hex string. String of hexadecimal digits. Example: 0123456989abcdef
ip <IPV4_HOST>	Option object type: IP address. IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
one-byte <UINT8>	Option object type: one byte. Integer in the form: D OR 0xHH. Example: 123

<i>string</i>	Option object type: string.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>two-byte</i>	Option object type: two byte.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
value ip 192.168.168.168
```

Syntax

```
name <DHCP_OPTION_GROUP>
```

Mode

DHCP Option Group

Description

Set DHCP server option group name.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
name "LAN Specific DHCP Option"
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

DHCP Option Group

Description

Add DHCP server option object to group.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
option object "LAN Specific DHCP Option"
```

Syntax

```
no option object <DHCP_OPTION_GROUP_OBJECT>
```

Mode

DHCP Option Group

Description

Remove DHCP server option object from group.

Options

<DHCP_OPTION_GROUP_OBJECT> DHCP server option object name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option object "LAN Specific DHCP Option"
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

DHCP Option Group

Description

Add DHCP server option group to group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group group1
```

Syntax

```
no option group <DHCP_OPTION_GROUP_GROUP>
```

Mode

DHCP Option Group

Description

Remove DHCP server option group from group.

Options

<DHCP_OPTION_GROUP_GROUP> DHCP server option group name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option group group1
```

Syntax

```
no members
```

Mode

DHCP Option Group

Description

Remove all DHCP server option members from group.

Example

```
no members
```

Syntax

```
clear failover-lb [ ipv4 | ipv6 ] statistics
```

Mode

All Modes
Top Level

Description

Reset failover and load balancing statistics.

Options

<i>ipv4</i>	Reset interface IPv4 statistics.
<i>ipv6</i>	Reset interface IPv6 statistics.
<i>statistics</i>	Reset failover and load balancing statistics.

Example

```
clear failover-lb statistics
```

Syntax

```
failover-lb
```

Mode

Config

Description

Enter failover and load balancing configuration mode.

Example

```
failover-lb
```

Syntax

```
enable
```

Mode

Failover & LB

Description

Enable failover and load balancing.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Failover & LB

Description

Disable failover and load balancing.

Example

no enable

Syntax

respond-to-probes

Mode

Failover & LB

Description

Enable respond to probes.

Example

respond to probes

Syntax

no respond-to-probes

Mode

Failover & LB

Description

Disable respond to probes.

Example

no respond to probes

Syntax

any-tcp-syn

Mode

Failover & LB

Description

Enable any-tcp-syn.

Example

any-tcp-syn

Syntax

no any-tcp-syn

Mode

Failover & LB

Description

Disable any-tcp-syn.

Example

no any-tcp-syn

Syntax

```
port <IPV4_PORT>
```

Mode

Failover & LB

Description

Set port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 8080
```

Syntax

```
group <FLB_GROUP_NAME>
```

Mode

Failover & LB

Description

Add/Edit load balancing group.

Options

<FLB_GROUP_NAME> Failover & LB group name.
Example: *myFLBGroup*

Example

```
group " Default LB Group"
```

Syntax

```
type { basic | ratio | round-robin | spillover }
```

Mode

LB Group

Description

Configure failover and load balancing type.

Options

<i>basic</i>	Connection use primary member unless failover occurs.
<i>ratio</i>	Connections use members according to the set percentages.
<i>round-robin</i>	Connections cycle through members in round robin fashion.
<i>spillover</i>	Connections use primary member until bandwidth is exceeded.

Example

```
type round-robin
```

Syntax

preempt

Mode

LB Group

Description

Enable preempt and failback to preferred member when possible.

Example

preempt

Syntax

no preempt

Mode

LB Group

Description

Disable preempt and failback to preferred member when possible.

Example

no preempt

Syntax

spillover-bandwidth <UINT32>

Mode

LB Group

Description

Set the bandwidth at which spill-over occurs in Kbps.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

spillover-bandwidth 1000

Syntax

no spillover-bandwidth

Mode

LB Group

Description

Clear the bandwidth at which spill-over occurs in Kbps.

Example

no spillover-bandwidth

Syntax

address-binding

Mode

LB Group

Description

Enable use source and destination IP address binding.

Example

address-binding

Syntax

no address-binding

Mode

LB Group

Description

Disable use source and destination IP address binding.

Example

no address-binding

Syntax

auto-adjust-ratio

Mode

LB Group

Description

Automatically adjust all member ratios so total is 100%.

Example

auto-adjust-ratio

Syntax

interface <FLB_GROUP_MEMBER>

Mode

LB Group

Description

Edit interface load balancing group member.

Options

<FLB_GROUP_MEMBER> WAN interface name.
Example: *X0*

Example

interface X2

Syntax

```
no interface <FLB_CURRENT_GROUP_MEMBER>
```

Mode

LB Group

Description

Remove interface load balancing group member.

Options

<FLB_CURRENT_GROUP_MEMBER> Group member name.
Example: *X0*

Example

```
no interface X2
```

Syntax

```
no interfaces
```

Mode

LB Group

Description

Remove all interface load balancing group member.

Example

```
no interfaces
```

Syntax

```
final-backup <FLB_FINAL_BACKUP>
```

Mode

LB Group

Description

Add/Replace final backup interface in load balancing group.

Options

<FLB_FINAL_BACKUP> WAN interface name.
Example: *X0*

Example

```
final-backup X4
```

Syntax

```
no final-backup
```

Mode

LB Group

Description

Remove final backup interface in load balancing group.

Example

```
no final-backup
```

Syntax

```
probing
```

Mode

LB Group

Description

Enter probing configuration mode.

Example

```
probing
```

Syntax

```
health-check <UINT16>
```

Mode

Probing

Description

Set the interval to perform health check of member (logical probing, physical link-check) in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
health-check 5
```

Syntax

```
missed-intervals <UINT16>
```

Mode

Probing

Description

Set the number of intervals to deactivate the member after.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
missed-intervals 6
```

Syntax

```
successful-intervals <UINT16>
```

Mode

Probing

Description

Set the number of intervals to reactivate the member after.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
successful-intervals 3
```

Syntax

```
global-responder
```

Mode

Probing

Description

Enable probing on all members using SonicWall's global responder.

Example

```
global-responder
```

Syntax

```
no global-responder
```

Mode

Probing

Description

Disable probing on all members using SonicWall's global responder and set to physical monitoring only.

Example

```
no global-responder
```

Syntax

```
rank <UINT32>
```

Mode

LB Group Member

Description

Interface rank.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
rank 2
```

Syntax

```
percent <FLB_CURRENT_GROUP_MEMBER> <UINT8>
```

Mode

LB Group

Description

Set the member usage percent for the interface.

Options

<FLB_CURRENT_GROUP_MEMBER>	Group member name. Example: <i>X0</i>
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

```
percent X1 55
```

Syntax

```
probe-type { logical | physical }
```

Mode

LB Group Member

Description

Configure probing type.

Options

logical	Use logical/probe monitoring.
physical	Use only physical checking of member status, no probing.

Example

```
probe-type logical
```

Syntax

```
probe-condition { always | both | either | main }
```

Mode

LB Group Member

Description

Configure under what condition probes succeed.

Options

always	Always succeeds (no probing).
both	Probes succeed when both main target and alternate target respond.
either	Probes succeed when either main target or alternate target responds.

main Probes succeed when main target responds.

Example

probe-condition either

Syntax

main-target [protocol { ping | tcp <IPV4_PORT> }] [host <HOSTNAME_MIXED>]

Mode

LB Group Member

Description

Configure main target probe settings.

Options

- protocol** Set the probe protocol.
- ping** Ping probes.
- tcp** TCP SYN probes.
- <IPV4_PORT>** Integer in the form: D OR 0xHHHH.
Example: 80
- host** Target name or IP address.
- <HOSTNAME_MIXED>** IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

main-target protocol tcp 8080 host 192.168.168.254
main-target protocol tcp 8080 host fe00::1

Syntax

no main-target protocol tcp

Mode

LB Group Member

Description

Clear main target probe protocol tcp port.

Options

- protocol** Set the probe protocol.
- tcp** TCP SYN probes.

Example

no main-target protocol tcp

Syntax

alternate-target [protocol { ping | tcp <IPV4_PORT> }] [host <HOSTNAME_MIXED>]

Mode

LB Group Member

Description

Configure alternate target probe settings.

Options

<i>protocol</i>	Set the probe protocol.
<i>ping</i>	Ping probes.
<i>tcp</i>	TCP SYN probes.
<i><IPV4_PORT></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>host</i>	Target Name or IP address.
<i><HOSTNAME_MIXED></i>	IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

```
alternate-target protocol tcp 8080 host 192.168.168.253
alternate-target protocol tcp 8080 host fe00::1
```

Syntax

```
no alternate-target protocol tcp
```

Mode

LB Group Member

Description

Clear alternate target probe tcp port.

Options

<i>protocol</i>	Set the probe protocol.
<i>tcp</i>	TCP SYN probes.

Example

```
no alternate-target protocol tcp
```

Syntax

```
default-target <IP_V4V6_HOST>
```

Mode

LB Group Member

Description

Configure the default target.

Options

<i><IP_V4V6_HOST></i>	IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>

Example

```
default-target 192.168.168.254
default-target fe00::1
```

Syntax

```
no default-target
```

Mode

LB Group Member

Description

Clear the default target.

Example

no default-target

Syntax

ip-helper

Mode

Config

Description

Configure IP helper.

Example

ip-helper

Syntax

enable

Mode

IP Helper

Description

Enable IP helper.

Example

enable

Syntax

no enable

Mode

IP Helper

Description

Disable IP helper.

Example

no enable

Syntax

policy protocol <IPH_PROTOCOL> source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> }

Mode

IP Helper

Description

Add/Edit IP helper policy.

Options

protocol <IPH_PROTOCOL>	Specify the IP helper relay protocol. IP Helper relay protocol name. Example: <i>mydns</i>
source	Specify source.
group <ADDR_GROUP_NAME>	IP helper policy source address object group. Group address object name. Example: <i>Sales Group</i>
interface <IPH_INTERFACE>	IP helper policy source interface. IP helper interface name. Example: <i>X1</i>
name <ADDR_NETWORK_NAME>	IP helper policy source address object name. Network address object name. Example: <i>Sales Network</i>
network <ADDR_NETWORK>	IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
zone <ZONE_NO_MULTICAST_NAME>	IP helper policy source zone. Zone object name. Example: <i>DMZ</i>

Example

policy protocol netBIOS source name "X0 Subnet"

Syntax

no policy protocol <IPH_PROTOCOL> source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> }

Mode

IP Helper

Description

Delete IP helper policy.

Options

protocol <IPH_PROTOCOL>	Specify the IP helper relay protocol. IP Helper relay protocol name. Example: <i>mydns</i>
source	Specify source.
group <ADDR_GROUP_NAME>	IP helper policy source address object group. Group address object name. Example: <i>Sales Group</i>
interface <IPH_INTERFACE>	IP helper policy source interface. IP helper interface name. Example: <i>X1</i>
name <ADDR_NETWORK_NAME>	IP helper policy source address object name. Network address object name. Example: <i>Sales Network</i>
network <ADDR_NETWORK>	IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>

<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
zone	IP helper policy source zone.
<ZONE_NO_MULTICAST_NAME>	Zone object name. Example: <i>DMZ</i>

Example

```
no policy protocol netBIOS source "Interface X0"
```

Syntax

```
no policies
```

Mode

IP Helper

Description

Delete all IP helper Policies.

Example

```
no policies
```

Syntax

```
protocol { enable | name } <IPH_PROTOCOL>
```

Mode

IP Helper

Description

Add/Edit IP helper protocol.

Options

enable	Enable specified IP helper relay protocol.
name	IP helper relay protocol name.
<IPH_PROTOCOL>	IP Helper relay protocol name. Example: <i>mydns</i>

Example

```
protocol name mydns
```

Syntax

```
no protocol { enable | name } <IPH_PROTOCOL>
```

Mode

IP Helper

Description

Delete IP helper relay protocol.

Options

enable	Enable IP Helper settings or objects.

<i>name</i>	IP helper relay protocol name.
<i><IPH_PROTOCOL></i>	IP Helper relay protocol name. Example: <i>mydns</i>

Example

no protocol name mydns

Syntax

no protocols

Mode

IP Helper

Description

Delete all IP helper relay protocols.

Example

no protocols

Syntax

enable

Mode

IP Helper Policy

Description

Enable IP helper policy.

Example

enable

Syntax

no enable

Mode

IP Helper Policy

Description

Disable IP helper policy.

Example

no enable

Syntax

protocol <IPH_PROTOCOL>

Mode

IP Helper Policy

Description

Specify IP helper relay protocol associated with this policy.

Options

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

protocol mydns

Syntax

source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> | name <ADDR_NETWORK_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | zone <ZONE_NO_MULTICAST_NAME> }

Mode

IP Helper Policy

Description

Specify source zone or interface for IP helper policy.

Options

group <ADDR_GROUP_NAME>	IP helper policy source address object group. Group address object name. Example: <i>Sales Group</i>
interface <IPH_INTERFACE>	IP helper policy source interface. IP helper interface name. Example: <i>X1</i>
name <ADDR_NETWORK_NAME>	IP helper policy source address object name. Network address object name. Example: <i>Sales Network</i>
network <ADDR_NETWORK>	IP helper policy source network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
zone <ZONE_NO_MULTICAST_NAME>	IP helper policy source zone. Zone object name. Example: <i>DMZ</i>

Example

source Interface X0

Syntax

destination { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | ipv6 <IPV6_HOST> | name <ADDR_IPH_POLICY_DST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> }

Mode

IP Helper Policy

Description

Specify IP helper policy destination.

Options

group Destination address object group name.

<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Destination address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
ipv6 <IPv6_HOST>	IPv6 helper policy destination. IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
name <ADDR_IPH_POLICY_DST_NAME>	Destination address object name. Host or network address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	IP helper policy destination network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>

Example

```
destination name "mydest"
destination ipv6 1::1
```

Syntax

```
comment <WORD>
```

Mode

IP Helper Policy

Description

Specify comment for IP helper policy.

Options

```
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
```

Example

```
comment "Need to allow NetBIOS between clients"
```

Syntax

```
no comment
```

Mode

IP Helper Policy

Description

Clear comment for IP helper policy.

Example

```
no comment
```

Syntax

```
egressif <IPH_INTERFACE>
```

Mode

IP Helper Policy

Description

Specify IPv6 helper policy egressif.

Options

<IPH_INTERFACE> IP helper interface name.
Example: *X1*

Example

Set Egress Interface

Syntax

no egressif

Mode

IP Helper Policy

Description

Clear IPv6 helper policy egressif.

Example

no egressif

Syntax

name <IPH_PROTOCOL>

Mode

IP Helper Protocol

Description

Specify IP Helper relay protocol name.

Options

<IPH_PROTOCOL> IP Helper relay protocol name.
Example: *mydns*

Example

name mydns

Syntax

enable

Mode

IP Helper Protocol

Description

Enable IP helper relay protocol.

Example

enable

Syntax

no enable

Mode

IP Helper Protocol

Description

Disable IP helper relay protocol.

Example

no enable

Syntax

no port1

Mode

IP Helper Protocol

Description

Clear IP helper relay protocol beginning UDP port.

Example

no port1

Syntax

port1 <IPV4_PORT>

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol beginning UDP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

port1 53

Syntax

no port2

Mode

IP Helper Protocol

Description

Clear IP helper relay protocol ending UDP port.

Example

no port2

Syntax

port2 <IPV4_PORT>

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol ending UDP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

port2 54

Syntax

timeout { 10 | 20 | 30 | 40 | 50 | 60 }

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol timeout.

Options

10 Timeout value (in seconds).

20 Timeout value (in seconds).

30 Timeout value (in seconds).

40 Timeout value (in seconds).

50 Timeout value (in seconds).

60 Timeout value (in seconds).

Example

timeout 20

Syntax

mode { both | broadcast | multicast }

Mode

IP Helper Protocol

Description

Specify IP helper relay protocol mode.

Options

both IP helper relay protocol broadcast mode.

broadcast IP helper relay protocol broadcast mode.

multicast IP helper relay protocol multicast mode.

Example

```
mode broadcast
```

Syntax

```
multicast-ip <IPV4_HOST>
```

Mode

IP Helper Protocol

Description

Specify Ip helper multicast address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
multicast-ip 1.1.1.1
```

Syntax

```
no multicast-ip
```

Mode

IP Helper Protocol

Description

Clear Ip helper multicast address.

Example

```
no multicast-ip
```

Syntax

```
multicast-ipv6 <IPV6_HOST> <IPV6_HOST>
```

Mode

IP Helper Protocol

Description

Specify Ipv6 helper multicast address.

Options

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

multicast-ipv6 FF02::1:2 FF05::1:3

Syntax

source-translation

Mode

IP Helper Protocol

Description

Allow IP source translation for IP helper relay protocol.

Example

source-translation

Syntax

no source-translation

Mode

IP Helper Protocol

Description

Enable allowing IP source translation for IP helper relay protocol.

Example

no source-translation

Syntax

raw

Mode

IP Helper Protocol

Description

Enable raw mode for IP helper relay protocol.

Example

raw

Syntax

no raw

Mode

IP Helper Protocol

Description

Disable raw mode for IP helper relay protocol.

Example

no raw

Syntax

```
mac-ip-anti-spoof [ ipv6 ]
```

Mode

Config

Description

Configure MAC-IP anti-spoof settings.

Options

ipv6 Enter IPv6 MAC-IP anti-spoof configuration mode.

Example

```
mac-ip-anti-spoof
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Configure MAC-IP anti-spoof for the specified interface.

Options

<MAC_IP_ANTI_SPOOF_INTERFACE> MAC-IP anti-spoof interface.
Example: *X0*

Example

```
interface X1
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Configure IPv6 MAC-IP anti-spoof for the specified interface.

Options

<MAC_IP_ANTI_SPOOF_INTERFACE> MAC-IP anti-spoof interface.
Example: *X0*

Example

```
interface X1
```

Syntax

```
cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Add/edit an MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP>	MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:3257:9652</i>
<MAC_IP_ANTI_SPOOF_STATIC_MAC>	MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i>
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>	MAC-IP anti-spoof enabled static interface. Example: <i>X0</i>

Example

```
cache entry 10.10.10.10 00:01:02:03:04:05 X0
```

Syntax

```
no cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof

Description

Delete an MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP>	MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:3257:9652</i>
<MAC_IP_ANTI_SPOOF_STATIC_MAC>	MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i>
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>	MAC-IP anti-spoof enabled static interface. Example: <i>X0</i>

Example

```
no cache entry 10.10.10.10 00:01:02:03:04:05 X0
no cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Add/edit an IPv6 MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP>	MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:3257:9652</i>
<MAC_IP_ANTI_SPOOF_STATIC_MAC>	MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i>
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>	MAC-IP anti-spoof enabled static interface. Example: <i>X0</i>

Example

```
cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
no cache entry <MAC_IP_ANTI_SPOOF_STATIC_IP> <MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof

Description

Delete an MAC-IP anti-spoof cache entry.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP>	MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:3257:9652</i>
<MAC_IP_ANTI_SPOOF_STATIC_MAC>	MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i>
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>	MAC-IP anti-spoof enabled static interface. Example: <i>X0</i>

Example

```
no cache entry 10.10.10.10 00:01:02:03:04:05 X0
no cache entry 1030::C9B4:FF12:48AA:1A2B 00:01:02:03:04:05 X0
```

Syntax

```
no cache entries [ ipv4 | ipv6 ]
```

Mode

MAC Anti-Spoof
IPv6 MAC Anti-Spoof

Description

Delete all MAC-IP anti-spoof cache entries.

Options

- ipv4** Delete all MAC-IP anti-spoof IPv4 cache entries.
- ipv6** Delete all MAC-IP anti-spoof IPv6 cache entries.

Example

```
no cache entries
```

Syntax

```
router
```

Mode

MAC Anti-Spoof Cache

Description

Device is a router(a network exist behind this device).

Example

```
router
```

Syntax

```
no router
```

Mode

MAC Anti-Spoof Cache

Description

Device is not a router.

Example

no router

Syntax

blacklisted

Mode

MAC Anti-Spoof Cache

Description

Device is blacklisted.

Example

blacklisted

Syntax

no blacklisted

Mode

MAC Anti-Spoof Cache

Description

Device is not blacklisted.

Example

no blacklisted

Syntax

ip <MAC_IP_ANTI_SPOOF_STATIC_IP>

Mode

MAC Anti-Spoof Cache

Description

IP address.

Options

<MAC_IP_ANTI_SPOOF_STATIC_IP> MAC-IP anti-spoof static ip.
Example: *2001:cdba:0000:0000:0000:3257:9652*

Syntax

mac <MAC_IP_ANTI_SPOOF_STATIC_MAC>

Mode

MAC Anti-Spoof Cache

Description

MAC address.

Options

<MAC_IP_ANTI_SPOOF_STATIC_MAC> MAC-IP anti-spoof static mac.
Example: *00:0C:F1:56:98:AD*

Syntax

```
interface <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

MAC Anti-Spoof Cache

Description

Interface.

Options

<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> MAC-IP anti-spoof enabled static interface.
Example: *X0*

Syntax

```
clear mac-ip-anti-spoof cache statistics ipv4
```

Mode

Top Level
Config
MAC Anti-Spoof

Description

Clear MAC-IP anti-spoof cache statistics.

Example

```
clear mac-ip-anti-spoof cache statistics ipv4
```

Syntax

```
clear mac-ip-anti-spoof spoof-detected-list ipv4
```

Mode

Top Level
Config
MAC Anti-Spoof

Description

Clear the whole spoof detected list.

Example

```
clear mac-ip-anti-spoof spoof-detected-list ipv4
```

Syntax

```
resolve mac-ip-anti-spoof spoof-detected-list ipv4
```

Mode

Description

Resolve names for the whole spoof detected list.

Example

```
resolve mac-ip-anti-spoof spoof-detected-list ipv4
```

Syntax

```
router
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is a router(a network exist behind this device).

Example

```
router
```

Syntax

```
no router
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is not a router.

Example

```
no router
```

Syntax

```
blacklisted
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is blacklisted.

Example

```
blacklisted
```

Syntax

```
no blacklisted
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Device is not blacklisted.

Example

```
no blacklisted
```

Syntax

```
ip <MAC_IP_ANTI_SPOOF_STATIC_IP>
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

IP address.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_IP>  MAC-IP anti-spoof static ip.  
Example: 2001:cdba:0000:0000:0000:3257:9652
```

Syntax

```
mac <MAC_IP_ANTI_SPOOF_STATIC_MAC>
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

MAC address.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_MAC>  MAC-IP anti-spoof static mac.  
Example: 00:0C:F1:56:98:AD
```

Syntax

```
interface <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>
```

Mode

IPv6 MAC Anti-Spoof Cache

Description

Interface.

Options

```
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>  MAC-IP anti-spoof enabled static interface.  
Example: X0
```

Syntax

```
clear mac-ip-anti-spoof cache statistics ipv6
```

Mode

Top Level
Config
IPv6 MAC Anti-Spoof

Description

Clear IPv6 MAC-IP anti-spoof cache statistics.

Example

```
clear mac-ip-anti-spoof cache statistics ipv6
```

Syntax

```
clear mac-ip-anti-spoof spoof-detected-list ipv6
```

Mode

Top Level
Config
IPv6 MAC Anti-Spoof

Description

Clear the whole IPv6 spoof detected list.

Example

```
clear mac-ip-anti-spoof spoof-detected-list ipv6
```

Syntax

```
resolve mac-ip-anti-spoof spoof-detected-list ipv6
```

Mode

Top Level
Config
IPv6 MAC Anti-Spoof

Description

Resolve names for the whole IPv6 spoof detected list.

Example

```
resolve mac-ip-anti-spoof spoof-detected-list ipv6
```

Syntax

```
enable
```

Mode

MAC Anti-Spoof IF

Description

Enable MAC-IP based anti-spoofing on this interface.

Example

```
enable
```

Syntax

```
no enable
```

Mode

MAC Anti-Spoof IF

Description

Disable MAC-IP based anti-spoofing on this interface.

Example

```
no enable
```

Syntax

```
static-arp
```

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof from static ARP entries.

Example

```
static-arp
```

Syntax

```
no static-arp
```

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof from static ARP entries.

Example

```
no static-arp
```

Syntax

```
dhcp-server
```

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof entry from DHCP lease (SonicWall's DHCP server).

Example

```
dhcp-server
```

Syntax

```
no dhcp-server
```

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof entry from DHCP lease (SonicWall's DHCP server).

Example

```
no dhcp-server
```

Syntax

```
dhcp-relay
```

Mode

MAC Anti-Spoof IF

Description

Enable population of MAC-IP anti-spoof entry from DHCP lease (DHCP relay - IP helper).

Example

```
dhcp-relay
```

Syntax

```
no dhcp-relay
```

Mode

MAC Anti-Spoof IF

Description

Disable population of MAC-IP anti-spoof entry from DHCP lease (DHCP relay - IP helper).

Example

```
no dhcp-relay
```

Syntax

```
arp-lock
```

Mode

MAC Anti-Spoof IF

Description

Enable locking of MAC-IP binding in ARP cache to prevent ARP poisoning from others.

Example

```
arp-lock
```

Syntax

```
no arp-lock
```

Mode

MAC Anti-Spoof IF

Description

Disable locking of MAC-IP binding in ARP cache.

Example

```
no arp-lock
```

Syntax

```
arp-watch
```

Mode

MAC Anti-Spoof IF

Description

Enable prevention of ARP poisoning of connected machines.

Example

```
arp-watch
```

Syntax

```
no arp-watch
```

Mode

MAC Anti-Spoof IF

Description

Disable prevention of ARP poisoning of connected machines.

Example

```
no arp-watch
```

Syntax

```
enforce-ingress
```

Mode

MAC Anti-Spoof IF

Description

Enable enforcement of ingress anti-spoof - drop packets not matching MAC-IP anti-spoof cache.

Example

```
enforce-ingress
```

Syntax

```
no enforce-ingress
```

Mode

MAC Anti-Spoof IF

Description

Disable enforcement of ingress anti-spoof.

Example

```
no enforce-ingress
```

Syntax

spoof-detection

Mode

MAC Anti-Spoof IF

Description

Enable creation of MAC-IP spoof detected list for packets failing to match anti-spoof cache.

Example

spoof-detection

Syntax

no spoof-detection

Mode

MAC Anti-Spoof IF

Description

Disable creation of MAC-IP spoof detected list for packets failing to match anti-spoof cache.

Example

no spoof-detection

Syntax

allow-management

Mode

MAC Anti-Spoof IF

Description

Enable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

allow-management

Syntax

no allow-management

Mode

MAC Anti-Spoof IF

Description

Disable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

no allow-management

Syntax

enable

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable MAC-IP based anti-spoofing on this interface.

Example

enable

Syntax

no enable

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable MAC-IP based anti-spoofing on this interface.

Example

no enable

Syntax

static-ndp

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable population of IPv6 MAC-IP anti-spoof from static NDP entries.

Example

static-ndp

Syntax

no static-ndp

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable population of IPv6 MAC-IP anti-spoof from static NDP entries.

Example

no static-ndp

Syntax

ndp-lock

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable locking of IPv6 MAC-IP binding in NDP cache to prevent NDP poisoning from others.

Example

```
ndp-lock
```

Syntax

```
no ndp-lock
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable locking of IPv6 MAC-IP binding in NDP cache.

Example

```
no ndp-lock
```

Syntax

```
enforce-ingress
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable enforcement of ingress anti-spoof - drop packets not matching MAC-IP anti-spoof cache.

Example

```
enforce-ingress
```

Syntax

```
no enforce-ingress
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable enforcement of ingress anti-spoof.

Example

```
no enforce-ingress
```

Syntax

```
spoof-detection
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable creation of MAC-IP spoof detected list for packets failing to match anti-spoof cache.

Example

```
spoof-detection
```

Syntax

```
no spoof-detection
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable creation of MAC-IP spoof detected list for packets failing to match anti-spoof cache.

Example

```
no spoof-detection
```

Syntax

```
allow-management
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Enable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
allow-management
```

Syntax

```
no allow-management
```

Mode

IPv6 MAC Anti-Spoof Interface

Description

Disable all traffic destined to the box to be allowed without a valid MAC-IP anti-spoof cache.

Example

```
no allow-management
```

Syntax

```
no nat-policy ipv4 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] ]
```


Mode

Config

Description

Delete a NAT policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
source	Original source ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source ("Original" if not specified).
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.

range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Original destination ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

<ADDR_END>	Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
translated-service	Translated service ("Original" if not specified).
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
original	Original service.
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
no nat-policy ipv4 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public"
translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
no nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group
<ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> |
range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host
<ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service
{ { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PROTOCOL> <SVC_PORT_BEGIN> }
} ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>
<SVC_PORT_END> } } ]
```

Mode

Config

Description

Delete an IPv6 NAT policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
source	Original source ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source ("Original" if not specified).
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Original destination ("Any" if not specified).

any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.

<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
translated-service	Translated service (\\"Original\\" if not specified).
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
original	Original service.
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
no nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public"
translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
no nat-policy ipv4 uuid <UUID>
```

Mode

Config

Description

Delete a NAT policy by associated UUID.

Options

<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>

Example

```
no nat-policy ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no nat-policy ipv6 uuid <UUID>
```

Mode

Config

Description

Delete an IPv6 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: 138a224d-c4c7-d621-0a00-c0eae49ce84c

Example

no nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no nat-policies [ipv4 | ipv6 | nat64]

Mode

Config

Description

Delete all NAT policies.

Options

ipv4 Delete all IPv4 NAT policies.

ipv6 Delete all IPv6 NAT policies.

nat64 Delete all NAT64 policies.

Example

no nat-policies

Syntax

nat-policy ipv4 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [source { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }] [translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }] [destination { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }] [translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }] [service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }] [translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }] [primitive]

Mode

Config

Description

Add/edit a NAT policy and enter its configuration mode.

Options

<NAT_INTERFACE> Interface name.
Example: X0

outbound Outbound interface.

<NAT_INTERFACE> Interface name.
Example: X0

source Original source ("Any" if not specified).

any Any host.

fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source ("Original" if not specified).
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Original destination ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.

<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>

protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
translated-service	Translated service ("Original" if not specified).

group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>

name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>

original	Original service.

protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
primitive	Configure a primitive NAT policy in one-line.

Example

```
nat-policy ipv4 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit an IPv6 NAT policy and enter its configuration mode.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
source	Original source ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_FHNR_NAME_WITH_MIXED> FQDN/host/network/range address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

translated-source Translated source ("Original" if not specified).

group Address object group.

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name Address object name.

<ADDR_NAME> Address object name.
Example: *Web Server*

network Address object network.

<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

original Original source IP.

range Address object range.

<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

destination Original destination ("Any" if not specified).

any Any host.

fqdn FQDN.

<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address object group.

<ADDR_FHNR_GROUP_WITH_MIXED> FQDN/host/network/range group address object name.
Example: *Web Server Group*

host Address object host.

<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

<i>translated-service</i>	Translated service (\\"Original\\" if not specified).
<i>group</i>	Service group.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<i><SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>
<i>original</i>	Original service.
<i>protocol</i>	Service object protocol.
<i><SVC_PROTOCOL></i>	Service protocol. Example: <i>TCP</i>
<i><SVC_PORT_BEGIN></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i><SVC_PORT_END></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>primitive</i>	Configure a primitive IPv6 NAT policy in one-line.

Example

```
nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
nat-policy ipv4 uuid <UUID>
```

Mode

Config

Description

Edit a NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
nat-policy ipv6 uuid <UUID>
```

Mode

Config

Description

Edit an IPv6 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group
<ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> |
range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ pref64 { { any | group <ADDR_GROUP_NAME>
| name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } } ] [ translated-destination { { embedded-ipv4-address | group
<ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN>
<ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL>
<SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol
<SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ]
```

Mode

Config

Description

Delete a NAT64 policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
source	IPv6 original source.
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated IPv4 source.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
pref64	NAT64 prefix.
any	Any host.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
translated-destination	Translated destination.
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

<i>service</i>	Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i> Original service.
<i>any</i>	Any service.
<i>group</i> <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>
<i>icmp-udp-tcp</i>	ICMP UDP TCP service.
<i>name</i> <SVC_NAME>	Service object name. Service object name. Example: <i>HTTPS</i>
<i>protocol</i> <SVC_PROTOCOL>	Service object protocol. Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>translated-service</i>	Translated service.
<i>group</i> <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>
<i>name</i> <SVC_NAME>	Service object name. Service object name. Example: <i>HTTPS</i>
<i>original</i>	Original service.
<i>protocol</i> <SVC_PROTOCOL>	Service object protocol. Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
no nat-policy nat64 inbound any outbound any source any translated-source X1 pref64 name nat64AO translated-destination
embedded-ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
no nat-policy nat64 uuid <UUID>
```

Mode

Config

Description

Delete a NAT64 policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```


Syntax

```
nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ source { { any | fqdn <ADDR_FQDN> | group
<ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> |
range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ pref64 { { any | group <ADDR_GROUP_NAME>
| name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } } ] [ translated-destination { { embedded-ipv4-address | group
<ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN>
<ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL>
<SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol
<SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit a NAT64 policy and enter its configuration mode.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
source	IPv6 original source.
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated IPv4 source.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
pref64	NAT64 prefix.
any	Any host.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
translated-destination	Translated destination.
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service.
any	Any service.

group Service group.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

icmp-udp-tcp ICMP UDP TCP service.

name Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

translated-service Translated service.

group Service group.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*

name Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*

original Original service.

protocol Service object protocol.
<SVC_PROTOCOL> Service protocol.
Example: *TCP*

<SVC_PORT_BEGIN> Integer in the form: D OR 0xHHHH.
Example: *80*

<SVC_PORT_END> Integer in the form: D OR 0xHHHH.
Example: *80*

primitive Configure a primitive NAT64 policy in one-line.

Example

```
nat-policy nat64 inbound any outbound any source any translated-source X1 pref64 name nat64AO translated-destination embedded-  
ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
nat-policy nat64 uuid <UUID>
```

Mode

Config

Description

Edit an NAT64 NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

uuid <UUID>

Mode

NAT

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

NAT

Description

Clear nat policy UUID.

Example

no uuid

Syntax

uuid <UUID>

Mode

IPv6 NAT

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

IPv6 NAT

Description

Clear nat policy UUID.

Example

no uuid

Syntax

uuid <UUID>

Mode

NAT64 Policy

Description

Nat policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

NAT64 Policy

Description

Clear nat policy UUID.

Example

no uuid

Syntax

name <WORD>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Nat policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name OfficeNatPolicy

Syntax

no name

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear NAT policy name.

Example

name OfficeNatPolicy

Syntax

priority { auto | manual <UINT32> }

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Set NAT policy priority.

Options

- auto** Set auto priority(priority = 0) for NAT policy.
- manual** Set manual priority for NAT policy.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

priority auto
priority manual 1

Syntax

comment <WORD>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify a comment for this NAT policy.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

comment "Public HTTP Server"

Syntax

no comment

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear NAT policy comment.

Example

no comment

Syntax

enable

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Enable NAT policy.

Example

enable

Syntax

no enable

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Disable NAT policy.

Example

no enable

Syntax

dns-doctoring

Mode

NAT

Description

Enable NAT policy DNS doctoring.

Example

dns-doctoring

Syntax

no dns-doctoring

Mode

NAT

Description

Disable NAT policy DNS doctoring.

Example

no dns-doctoring

Syntax

inbound <NAT_INTERFACE>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the inbound interface for the NAT policy.

Options

<NAT_INTERFACE> Interface name.
Example: *X0*

Example

inbound X1

Syntax

outbound <NAT_INTERFACE>

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the outbound interface for the NAT policy.

Options

<NAT_INTERFACE> Interface name.
Example: *X0*

Example

outbound X0

Syntax

destination { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }

Mode

NAT
IPv6 NAT

Description

Specify the original destination for the NAT policy.

Options

<i>any</i>	Any host.
<i>fqdn</i> <ADDR_FQDN>	FQDN. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_FHNR_GROUP_WITH_MIXED>	Address object group. FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_FHNR_NAME_WITH_MIXED>	Address object name. FQDN/host/network/range address object name. Example: <i>Web Server</i>
<i>network</i> <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <ADDR_BEGIN> <ADDR_END>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

destination name "Web Server Public"

Syntax

source { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }

Mode

NAT
IPv6 NAT

Description

Specify the original source for the NAT policy.

Options

<i>any</i>	Any host.
<i>fqdn</i> <ADDR_FQDN>	FQDN. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i>	Address object group.

<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

source any

Syntax

```
service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>
<SVC_PORT_END> } }
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the original service for the NAT policy.

Options

any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

service name "My Web Services"

Syntax

reflexive

Mode

NAT
IPv6 NAT

Description

Configure a reflexive rule.

Example

reflexive

Syntax

no reflexive

Mode

NAT
IPv6 NAT

Description

Disable configuration of a reflexive rule.

Example

no reflexive

Syntax

translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the translated destination for the NAT policy.

Options

<i>embedded-ipv4-address</i>	Embedded ipv4 address.
<i>group</i>	Address object group.
<i><ADDR_GROUP_NAME></i>	Group address object name. Example: <i>Sales Group</i>
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<i><ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>
<i>network</i>	Address object network.

<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
translated-destination name "Web Server Private"
```

Syntax

```
translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT
IPv6 NAT

Description

Specify the translated source for the NAT policy.

Options

group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
translated-source original
```

Syntax

```
translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Specify the translated service for the NAT policy.

Options

group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
original	Original service.
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
translated-service original
```

Syntax

```
override-mac <MAC>
```

Mode

NAT

Description

Specify the override mac for the NAT policy.

Options

<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>

Example

```
override-mac 00:17:C5:0F:73:F4
```

Syntax

```
source { { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

NAT64 Policy

Description

Specify the original source for the NAT64 policy.

Options

<i>any</i>	Any host.
<i>fqdn</i> <ADDR_FQDN>	FQDN. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_FHNR_GROUP_WITH_MIXED>	Address object group. FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_FHNR_NAME_WITH_MIXED>	Address object name. FQDN/host/network/range address object name. Example: <i>Web Server</i>
<i>network</i> <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <ADDR_BEGIN> <ADDR_END>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

source any

Syntax

translated-source { { *group* <ADDR_GROUP_NAME> | *host* <ADDR_HOST> | *name* <ADDR_NAME> | *network* <ADDR_NETWORK> <ADDR_MASK> | *original* | *range* <ADDR_BEGIN> <ADDR_END> } }

Mode

NAT64 Policy

Description

Specify the translated source for the NAT64 policy.

Options

<i>group</i> <ADDR_GROUP_NAME>	Address object group. Group address object name. Example: <i>Sales Group</i>
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_NAME>	Address object name. Address object name. Example: <i>Web Server</i>

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
translated-source "X1 IP"
```

Syntax

```
pref64 { { any | group <ADDR_GROUP_NAME> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } }
```

Mode

NAT64 Policy

Description

Specify the prefix for the NAT64 policy.

Options

any	Any host.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>

Example

```
pref64 name nat64A0
```

Syntax

```
high-availability
```

Mode

NAT
IPv6 NAT

Description

NAT high availability and load balancing configuration mode.

Example

Syntax

```
nat-method { block-remap | random-distribution | round-robin | sticky-ip | symmetrical-remap }
```

Mode

NAT
IPv6 NAT

Description

Set the NAT destination translation method.

Options

<i>block-remap</i>	Block remap.
<i>random-distribution</i>	Random distribution.
<i>round-robin</i>	Round robin.
<i>sticky-ip</i>	Sticky IP.
<i>symmetrical-remap</i>	Symmetrical remap.

Example

```
nat-method sticky-ip
```

Syntax

```
source-port-remap
```

Mode

NAT
IPv6 NAT

Description

Enable source port remap.

Example

```
source-port-remap
```

Syntax

```
no source-port-remap
```

Mode

NAT
IPv6 NAT

Description

Disable source port remap.

Example

```
no source-port-remap
```

Syntax

probing

Mode

High Availability

Description

Enable HA probing and enter configuration mode.

Example

probing

Syntax

no probing

Mode

High Availability

Description

Disable HA probing.

Example

no probing

Syntax

probe-every <UINT16>

Mode

High Availability Probe

Description

Set probe interval (in seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

probe-every 5

Syntax

probe-type { *icmp-ping* | *tcp* <IPV4_PORT> }

Mode

High Availability Probe

Description

Set probe IP type.

Options

icmp-ping ICMP ping probe.

tcp	TCP probe.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: 80

Example

```
probe-type tcp 80
```

Syntax

```
reply-timeout <UINT16>
```

Mode

High Availability Probe

Description

Set reply timeout (in seconds).

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: 123

Example

```
reply-timeout 5
```

Syntax

```
deactivate-after <UINT16>
```

Mode

High Availability Probe

Description

Set number of missed probes required before deactivating the NAT policy.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: 123

Example

```
deactivate-after 4
```

Syntax

```
reactivate-after <UINT16>
```

Mode

High Availability Probe

Description

Set number of successful probes required before reactivating the NAT policy.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: 123

Example

reactivate-after 3

Syntax

rst-as-miss

Mode

High Availability Probe

Description

Enable count RST response as miss.

Example

rst-as-miss

Syntax

no rst-as-miss

Mode

High Availability Probe

Description

Disable count RST response as miss.

Example

no rst-as-miss

Syntax

port-probing

Mode

High Availability Probe

Description

Enable port probing.

Example

port-probing

Syntax

no port-probing

Mode

High Availability Probe

Description

Disable port probing.

Example

no port-probing

Syntax

```
ticket tag1 <WORD>
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Set ticket tag 1.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag1 "Tag number 1"
```

Syntax

```
no ticket tag1
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear ticket tag 1.

Example

```
no ticket tag1
```

Syntax

```
ticket tag2 <WORD>
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Set ticket tag 2.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag2 "Tag number 2"
```

Syntax

```
no ticket tag2
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear ticket tag 2.

Example

```
no ticket tag2
```

Syntax

```
ticket tag3 <WORD>
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Set ticket tag 3.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag3 "Tag number 3"
```

Syntax

```
no ticket tag3
```

Mode

NAT
NAT64 Policy
IPv6 NAT

Description

Clear ticket tag 3.

Example

```
no ticket tag3
```

Syntax

```
clear nat-policy statistics
```

Mode

Config

Description

Clear NAT policy statistics.

Example

```
clear nat-policy statistics
```

Syntax

```
no network-monitor policy [ ipv4 | ipv6 ] <NETMON_NAME>
```

Mode

Config

Description

Delete network monitor policy.

Options

ipv4	Delete IPv4 network monitor policy.
ipv6	Delete IPv6 network monitor policy.
<NETMON_NAME>	Atom Object name. Example: <i>Web Services Monitor</i>

Example

```
no network-monitor policy "Remote Servers"  
no network-monitor policy ipv6 "IPv6 Remote Servers"
```

Syntax

```
no network-monitor policies [ ipv6 ]
```

Mode

Config

Description

Delete all network monitor policies.

Options

ipv6	Delete IPv6 network monitor policies.

Example

```
no network-monitor policies  
no network-monitor policies ipv6
```

Syntax

```
clear network-monitor statistics
```

Mode

Config

Description

Clear network monitor statistics.

Example

```
clear network-monitor statistics
```

Syntax

```
network-monitor policy [ ipv6 ] <NETMON_NAME>
```

Mode

Config

Description

Add/edit a network monitor policy.

Options

ipv6	Add/edit an IPv6 network monitor policy.
<NETMON_NAME>	Atom Object name. Example: <i>Web Services Monitor</i>

Example

```
network-monitor policy "Remote Servers"  
network-monitor policy ipv6 "IPv6 Remote Servers"
```

Syntax

```
name <NETMON_NAME>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Edit a network monitor policy name.

Options

<NETMON_NAME>	Atom Object name. Example: <i>Web Services Monitor</i>

Example

```
name "Remote Servers"
```

Syntax

```
no probe target
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear the probe target.

Example

```
no probe target
```

Syntax

```
probe target { fqdn <ADDR_FQDN> | group <ADDR_FHR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name  
<ADDR_FQDN_HOST_RANGE_NAME_WITH_MIXED> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the probe target.

Options

<i>fqdn</i> <ADDR_FQDN>	Set the probe target to FQDN address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_FHR_GROUP_WITH_MIXED>	Set the probe target to group address object. FQDN/host/range group address object name. Example: <i>Web Server Group</i>
<i>host</i> <ADDR_HOST>	Set the probe target to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_FQDN_HOST_RANGE_NAME_WITH_MIXED>	Set the probe target to named address object. FQDN/host/range address object name. Example: <i>Web Server</i>
<i>range</i> <ADDR_BEGIN> <ADDR_END>	Set the probe target to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

probe target name "Remote Target"

Syntax

next-hop { host <ADDR_HOST> | name <ADDR_HOST_NAME> }

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the next hop gateway.

Options

<i>host</i> <ADDR_HOST>	Set the next hop to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_HOST_NAME>	Set the next hop to named address object. Host address object name. Example: <i>Web Server</i>

Example

next-hop name "X1 Default Gateway"

Syntax

no next-hop

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear the next hop gateway.

Example

no next-hop

Syntax

local-ip { host <NETMON_HOST> | name <ADDR_HOST_NAME> }

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set the local IP address.

Options

<i>host</i>	Set the local IP to host address.
<i><NETMON_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Set the local IP to named address object.
<i><ADDR_HOST_NAME></i>	Host address object name. Example: <i>Web Server</i>

Example

local-ip name "X1 IP"

Syntax

no local-ip

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear the local IP address.

Example

no local-ip

Syntax

outbound-interface <NETMON_INTERFACE>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set outbound interface.

Options

<NETMON_INTERFACE> Interface name.
Example: *X0*

Example

outbound-interface X2

Syntax

probe type { ping [{ explicit | non-explicit }] | tcp { [explicit | non-explicit] port <IPV4_PORT> } }

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set network monitor policy probe type.

Options

- ping** Ping probe.
- explicit** Ping probe using explicit route.
- non-explicit** Ping probe.
- tcp** TCP probe.
- explicit** TCP probe using explicit route.
- non-explicit** TCP probe.
- port** Set TCP probe port.
- <IPV4_PORT>** Integer in the form: D OR 0xHHHH.
Example: *80*

Example

probe type ping
probe type ping explicit
probe type tcp explicit port 80
probe type tcp port 80

Syntax

probe interval <UINT16>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set probe host interval.

Options

- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

probe interval 5

Syntax

```
reply-timeout <UINT8>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set probing reply timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
reply-timeout 2
```

Syntax

```
interval missed <UINT8>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Probe state is set to DOWN after specified number of missed intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval missed 3
```

Syntax

```
interval successful <UINT8>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Probe state is set to UP after specified number of successful intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
interval successful 3
```

Syntax

```
must-respond
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Enable all hosts must respond.

Example

```
must-respond
```

Syntax

```
no must-respond
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Disable all hosts must respond.

Example

```
no must-respond
```

Syntax

```
rst-as-miss
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Enable RST response counts as miss.

Example

```
rst-as-miss
```

Syntax

```
no rst-as-miss
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Disable RST response counts as miss.

Example

```
no rst-as-miss
```

Syntax

```
comment <WORD>
```

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Set network monitor policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Remote Servers"

Syntax

no comment

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear network monitor policy comment.

Example

no comment

Syntax

uuid <UUID>

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Network monitor UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Network Monitor Policy
IPv6 Network Monitor Policy

Description

Clear network monitor UUID.

Example

```
no uuid
```

Syntax

```
routing
```

Mode

Config

Description

Enter routing configuration mode.

Example

```
routing
```

Syntax

```
mode { advanced | simple }
```

Mode

Routing

Description

Routing mode.

Options

advanced Advanced routing.

simple Simple RIP advertisement.

Example

```
mode simple
mode advanced
```

Syntax

```
nsm
```

Mode

Routing

Description

Configure network services module (NSM) protocol.

Example

```
nsm
```

Syntax

```
ospf
```

Mode

Routing

Description

Configure open shortest path first (OSPF) protocol.

Example

```
ospf
```

Syntax

```
rip
```

Mode

Routing

Description

Configure routing information protocol (RIP).

Example

```
rip
```

Syntax

```
ospfv3
```

Mode

Routing

Description

Configure Open Shortest Path First (OSPFv3) protocol.

Example

```
ospfv3
```

Syntax

```
ripng
```

Mode

Routing

Description

Configure Routing Information Protocol (RIPng).

Example

```
ripng
```

Syntax

```
no bgp
```

Mode

Routing

Description

Disable border gateway protocol (BGP).

Example

```
no bgp
```

Syntax

```
bgp
```

Mode

Routing

Description

Enable and configure border gateway protocol (BGP).

Example

```
bgp
```

Syntax

```
default-route-metric <UINT8>
```

Mode

Routing

Description

Set metric for default routes received from advanced routing protocols.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
default-route-metric 110
```

Syntax

```
metric-priority
```

Mode

Routing

Description

Enable prioritize routes by metric within route classes.

Example

```
metric-priority
```

Syntax

```
no metric-priority
```

Mode

Description

Disable prioritize routes by metric within route classes.

Example

```
no metric-priority
```

Syntax

```
no route-policy ipv4 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | application <APP_GROUP_NAME> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ tos <ROUTE_HEX_UINT8> ] [ mask <ROUTE_HEX_UINT8> ] [ distance { auto | value <UINT8> } ] [ path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME> ] [ nexthop-number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4 <ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ] ] ]
```

Mode

Config

Description

Delete a route policy.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
metric	Route policy metric.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
source	Route policy source.
any	Any host.
group <ADDR_GROUP_NAME>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name <ADDR_HOST_NETWORK_RANGE_NAME>	Address object name. Host/network/range address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Route policy destination.
any	Any host.

fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_WITH_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_FHNR_NAME_WITH_MIXED>	Address object name. FQDN/host/network/range address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN> <ADDR_END>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
app <ROUTING_POLICY_APP_MATCH_OBJECT>	Route policy application match-object. Route application match-object name. Example: <i>abc</i>
application <APP_GROUP_NAME>	set route policy application group. Atom Object name. Example: <i>Application Tech Apps</i>
service	Route policy service.
any	Any service.
group <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>
name <SVC_NAME>	Service object name. Service object name. Example: <i>HTTPS</i>
protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END>	Service object protocol. Service protocol. Example: <i>TCP</i> Integer in the form: D OR 0xHHHH. Example: <i>80</i> Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host <ADDR_HOST>	Gateway IP. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_HOST_NAME>	Address object name. Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.

<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
path-selection-profile	Route policy SD-WAN path selection profile.
<ROUTE_PATH_SELECTION_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
nexthop-number	the nexthop number.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
interface2	Route policy 2nd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway2	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
interface3	Route policy 3rd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway3	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
interface4	Route policy 4th interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway4	Route policy 4th gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

Example

```
no route-policy ipv4 interface X4 metric 255 service name "FTP" gateway default
```

Syntax

```
no route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host
<ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [
destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name
<ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app
<ROUTING_POLICY_APP_MATCH_OBJECT> | application <APP_GROUP_NAME> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME>
| protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name
<ADDR_HOST_NAME> } } ] [ tos <ROUTE_HEX_UINT8> ] [ mask <ROUTE_HEX_UINT8> ] [ distance { auto | value <UINT8> } ] [ nexthop-
number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [
interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface4
<ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ]
```

Mode

Config

Description

Delete an IPv6 route policy.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
metric	Route policy metric.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
source	Route policy source.
any	Any host.
group	Address group name.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Route policy destination.
any	Any host.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.

<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
app	Route policy application match-object.
<ROUTING_POLICY_APP_MATCH_OBJECT>	Route aplication match-object name. Example: <i>abc</i>
application	set route policy application group.
<APP_GROUP_NAME>	Atom Object name. Example: <i>Application Tech Apps</i>
service	Route policy service.
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
nexthop-number	the nexthop number.
<UINT8>	Integer in the form: D OR 0xHH.

<i>interface2</i>	Example: <i>123</i>
<ROUTING_INTERFACE_NAME>	Route policy 2nd interface. Route interface name. Example: <i>X0</i>
<i>gateway2</i>	Route policy 2nd gateway.
<i>default</i>	Default gateway 0.0.0.0/::
<i>host</i>	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
<i>interface3</i>	Route policy 3rd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
<i>gateway3</i>	Route policy 2nd gateway.
<i>default</i>	Default gateway 0.0.0.0/::
<i>host</i>	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
<i>interface4</i>	Route policy 4th interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
<i>gateway4</i>	Route policy 4th gateway.
<i>default</i>	Default gateway 0.0.0.0/::
<i>host</i>	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

Example

```
no route-policy ipv6 interface X4 metric 255 service name "FTP" gateway default
```

Syntax

```
no route-policy ipv4 uuid <UUID>
```

Mode

Config

Description

Delete a route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no route-policy ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no route-policy ipv6 uuid <UUID>
```

Mode

Config

Description

Delete an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no route-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no route-policies [ ipv4 | ipv6 ]
```

Mode

Config

Description

Delete all route policies.

Options

ipv4 Delete all IPv4 route policies.

ipv6 Delete all IPv6 route policies.

Example

```
no route-policies
no route-policies ipv4
no route-policies ipv6
```

Syntax

```
no route-policies-sdwan
```

Mode

Config
Routing

Description

Delete all SD-WAN route policies.

Example

```
no route-policies-sdwan
```

Syntax

```
no route-policies-ipv4
```

Mode

Config
Routing

Description

Delete all IPv4 route policies.

Example

```
no route-policies-ipv4
```

Syntax

```
no route-policies-ipv6
```

Mode

Config
Routing

Description

Delete all IPv6 route policies.

Example

```
no route-policies-ipv6
```

Syntax

```
route-policy ipv4 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | application <APP_GROUP_NAME> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ tos <ROUTE_HEX_UINT8> ] [ mask <ROUTE_HEX_UINT8> ] [ distance { auto | value <UINT8> } ] [ path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME> ] [ nexthop-number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4 <ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ] [ name <WORD> ] [ primitive ]
```

Mode

Config

Description

Add/edit a route policy.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
metric <UINT8>	Route policy metric. Integer in the form: D OR 0xHH. Example: <i>123</i>
source	Route policy source.
any	Any host.
group <ADDR_GROUP_NAME>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

<i>name</i>	Address object name.
<i><ADDR_HOST_NETWORK_RANGE_NAME></i>	Host/network/range address object name. Example: <i>Web Server</i>
<i>network</i>	Address object network.
<i><ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
<i>range</i>	Address object range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>destination</i>	Route policy destination.
<i>any</i>	Any host.
<i>fqdn</i>	Address object full qualified domain name.
<i><ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i>	Address group name.
<i><ADDR_GROUP_NAME_WITH_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<i><ADDR_FHNR_NAME_WITH_MIXED></i>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
<i>network</i>	Address object network.
<i><ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
<i>range</i>	Address object range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>app</i>	Route policy application match-object.
<i><ROUTING_POLICY_APP_MATCH_OBJECT></i>	Route application match-object name. Example: <i>abc</i>
<i>application</i>	set route policy application group.
<i><APP_GROUP_NAME></i>	Atom Object name. Example: <i>Application Tech Apps</i>
<i>service</i>	Route policy service.
<i>any</i>	Any service.
<i>group</i>	Service group.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>

name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
path-selection-profile	Route policy SD-WAN path selection profile.
<ROUTE_PATH_SELECTION_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
nexthop-number	the nexthop number.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
interface2	Route policy 2nd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway2	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
interface3	Route policy 3rd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway3	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

interface4	Route policy 4th interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway4	Route policy 4th gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
name	Set route policy name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
primitive	Configure a primitive route policy in one-line.

Example

```
route-policy ipv4 interface X4 metric 255 source any destination any service any gateway default
```

Syntax

```
route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ app <ROUTING_POLICY_APP_MATCH_OBJECT> | application <APP_GROUP_NAME> | service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ tos <ROUTE_HEX_UINT8> ] [ mask <ROUTE_HEX_UINT8> ] [ distance { auto | value <UINT8> } ] [ nexthop-number <UINT8> interface2 <ROUTING_INTERFACE_NAME> [ gateway2 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface3 <ROUTING_INTERFACE_NAME> [ gateway3 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] [ interface4 <ROUTING_INTERFACE_NAME> [ gateway4 { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] ] ] [ name <WORD> ] [ primitive ]
```

Mode

Config

Description

Add/edit an IPv6 route policy.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
metric	Route policy metric.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
source	Route policy source.
any	Any host.
group	Address group name.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

<ADDR_MASK>	Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Route policy destination.
any	Any host.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
app	Route policy application match-object.
<ROUTING_POLICY_APP_MATCH_OBJECT>	Route aplication match-object name. Example: <i>abc</i>
application	set route policy application group.
<APP_GROUP_NAME>	Atom Object name. Example: <i>Application Tech Apps</i>
service	Route policy service.
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
nexthop-number	the nexthop number.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
interface2	Route policy 2nd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway2	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
interface3	Route policy 3rd interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway3	Route policy 2nd gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
interface4	Route policy 4th interface.
<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
gateway4	Route policy 4th gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

<i>name</i>	Address object name.
<i><ADDR_HOST_NAME></i>	Host address object name. Example: <i>Web Server</i>
<i>name</i>	Set route policy name.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>primitive</i>	Configure a primitive IPv6 route policy in one-line.

Example

```
route-policy ipv6 interface X4 metric 255 source any destination any service any gateway default
```

Syntax

```
route-policy ipv4 uuid <UUID>
```

Mode

Config

Description

Edit a route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
route-policy ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
uuid <UUID>
```

Mode

Route Policy

Description

Route policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid 3824334935410777187
```

Syntax

```
no uuid
```

Mode

Route Policy

Description

Clear route policy UUID.

Example

no uuid

Syntax

route-policy ipv6 uuid <UUID>

Mode

Config

Description

Edit an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

route-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

uuid <UUID>

Mode

IPV6 Route Policy

Description

Route policy UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Route Policy

Description

Clear route policy UUID.

Example

no uuid

Syntax

```
source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy source.

Options

any	Any host.
group <ADDR_GROUP_NAME>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_HOST_NETWORK_RANGE_NAME>	Address object name. Host/network/range address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
source name "X0 Default Gateway"  
source group "Corp LAN2"  
source any
```

Syntax

```
destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy destination.

Options

any	Any host.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>

group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
destination name "X0 Default Gateway"
destination group "Corp LAN2"
destination any
```

Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy service.

Options

any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
service name "LAN Service"
```

Syntax

app <ROUTING_POLICY_APP_MATCH_OBJECT>

Mode

Route Policy
IPv6 Route Policy

Description

set route policy application match-object.

Options

<ROUTING_POLICY_APP_MATCH_OBJECT> Route application match-object name.
Example: *abc*

Example

app IM_App

Syntax

application <APP_GROUP_NAME>

Mode

Route Policy
IPv6 Route Policy

Description

set route policy application group.

Options

<APP_GROUP_NAME> Atom Object name.
Example: *Application Tech Apps*

Example

application "Severe Risk App Group"

Syntax

gateway { { *default* | *host* <ADDR_HOST> | *name* <ADDR_HOST_NAME> } }

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy gateway.

Options

<i>default</i>	Default gateway 0.0.0.0/::
<i>host</i>	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.

<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
tos <ROUTE_HEX_UINT8>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy TOS.

Options

<ROUTE_HEX_UINT8> Hexadecimal integer in the form: 0xHH.
Example: *0xaa*

Example

```
tos 22
```

Syntax

```
no tos
```

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy TOS.

Example

```
no tos
```

Syntax

```
mask <ROUTE_HEX_UINT8>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy TOS mask.

Options

<ROUTE_HEX_UINT8> Hexadecimal integer in the form: 0xHH.
Example: *0xaa*

Example

```
mask 22
```

Syntax

no mask

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy TOS mask.

Example

no mask

Syntax

distance { auto | value <UINT8> }

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy distance.

Options

- auto** Route policy auto admin distance.
- value** Route policy custom admin distance.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

Example

distance auto
distance value 10

Syntax

path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME>

Mode

Route Policy

Description

Set route policy SD-WAN path selection profile.

Options

- <ROUTE_PATH_SELECTION_PROFILE_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

path-selection-profile sdwanProfile

Syntax

no path-selection-profile

Mode

Route Policy

Description

Clear route policy SD-WAN path selection profile.

Example

```
no path-selection-profile
```

Syntax

```
interface <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: X0

Example

```
interface X2
```

Syntax

```
gateway2 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 2nd gateway.

Options

- default** Default gateway 0.0.0.0/::
- host** Gateway IP.
- <ADDR_HOST>** IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*
- name** Address object name.
- <ADDR_HOST_NAME>** Host address object name.
Example: *Web Server*

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
interface2 <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy 2nd interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

Example

interface X2

Syntax

gateway3 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy 3rd gateway.

Options

default Default gateway 0.0.0.0/::

host Gateway IP.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

name Address object name.
<ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

gateway name "X0 Default Gateway"
gateway default

Syntax

interface3 <ROUTING_INTERFACE_NAME>

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy 3rd interface.

Options

<ROUTING_INTERFACE_NAME> Route interface name.
Example: *X0*

Example

interface X2

Syntax

```
gateway4 { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> }
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy 4th gateway.

Options

default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

Example

```
gateway name "X0 Default Gateway"  
gateway default
```

Syntax

```
interface4 <ROUTING_INTERFACE_NAME>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route 4th policy interface.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>

Example

```
interface X2
```

Syntax

```
nexthop-number <UINT8>
```

Mode

Route Policy
IPv6 Route Policy

Description

Set route policy nexthop number.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

nexthop-number 2

Syntax

metric **<UINT8>**

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy metric.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

metric 1

Syntax

no name

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy name.

Example

no name

Syntax

name **<WORD>**

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Route to Corporate Servers"

Syntax

no comment

Mode

Route Policy
IPV6 Route Policy

Description

Clear route policy comment.

Example

no comment

Syntax

comment <WORD>

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Route to Corporate Servers"

Syntax

disable-on-interface-down

Mode

Route Policy
IPV6 Route Policy

Description

Disable route when the interface is disconnected.

Example

disable-on-interface-down

Syntax

no disable-on-interface-down

Mode

Route Policy
IPV6 Route Policy

Description

Leave route enabled when the interface is disconnected.

Example

no disable-on-interface-down

Syntax

vpn-precedence

Mode

Route Policy
IPV6 Route Policy

Description

Allow VPN path to take precedence.

Example

vpn-precedence

Syntax

no vpn-precedence

Mode

Route Policy
IPV6 Route Policy

Description

Disable allow VPN path to take precedence.

Example

no vpn-precedence

Syntax

tcp-acceleration

Mode

Route Policy

Description

Enable permit TCP acceleration.

Example

tcp-acceleration

Syntax

no tcp-acceleration

Mode

Route Policy

Description

Disable permit TCP acceleration.

Example

no tcp-acceleration

Syntax

wxa-group <WXA_GROUP_NAME>

Mode

Route Policy

Description

Configure WXA group.

Options

<WXA_GROUP_NAME> WXA group name.
Example: *Group One*

Example

wxa-group "Group One"

Syntax

no wxa-group

Mode

Route Policy

Description

Clear WXA group.

Example

no wxa-group

Syntax

auto-add-access-rules

Mode

Route Policy
IPV6 Route Policy

Description

Enable auto-add access rules.

Example

auto-add-access-rules

Syntax

no auto-add-access-rules

Mode

Route Policy
IPV6 Route Policy

Description

Disable auto-add access rules.

Example

```
no auto-add-access-rules
```

Syntax

```
probe <NETMON_NAME>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set route policy probing.

Options

<NETMON_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
probe Web-Servers
```

Syntax

```
no probe
```

Mode

Route Policy
IPV6 Route Policy

Description

Disable route policy probing.

Example

```
no probe
```

Syntax

```
disable-when-probes-succeed
```

Mode

Route Policy
IPV6 Route Policy

Description

Disable route when probe succeeds.

Example

```
disable-when-probes-succeed
```

Syntax

```
no disable-when-probes-succeed
```

Mode

Route Policy
IPV6 Route Policy

Description

Do not disable route when probe succeeds.

Example

```
no disable-when-probes-succeed
```

Syntax

```
default-probe-state-up
```

Mode

Route Policy
IPV6 Route Policy

Description

Set probe default state to up.

Example

```
default-probe-state-up
```

Syntax

```
no default-probe-state-up
```

Mode

Route Policy
IPV6 Route Policy

Description

Set probe default state to down.

Example

```
no default-probe-state-up
```

Syntax

```
ticket tag1 <WORD>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set ticket tag 1.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag1 myroute
```

Syntax

```
no ticket tag1
```

Mode

Route Policy
IPV6 Route Policy

Description

Clear ticket tag 1.

Example

```
no ticket tag1
```

Syntax

```
ticket tag2 <WORD>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set ticket tag 2.

Options

<**WORD**> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag2 myroute
```

Syntax

```
no ticket tag2
```

Mode

Route Policy
IPV6 Route Policy

Description

Clear ticket tag 2.

Example

```
no ticket tag2
```

Syntax

```
ticket tag3 <WORD>
```

Mode

Route Policy
IPV6 Route Policy

Description

Set ticket tag 3.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag3 myroute
```

Syntax

```
no ticket tag3
```

Mode

Route Policy
IPv6 Route Policy

Description

Clear ticket tag 3.

Example

```
no ticket tag3
```

Syntax

```
ipv6 default-route-metric <UINT8>
```

Mode

Routing

Description

Apply the metric to IPv6 default routes learned through router advertisement.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
ipv6 default-route-metric 20
```

Syntax

```
web-proxy
```

Mode

Config

Description

Set automatic proxy forwarding (web only).

Example

```
web-proxy
```

Syntax

```
server <HOSTNAME>
```

Mode

Web Proxy

Description

Set web proxy hostname/IP.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
server 10.10.10.100
```

Syntax

```
no server
```

Mode

Web Proxy

Description

Clear web proxy hostname/IP.

Example

```
no server
```

Syntax

```
port <UINT16>
```

Mode

Web Proxy

Description

Web proxy TCP port.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
port 4433
```

Syntax

```
no port
```

Mode

Web Proxy

Description

Clear web proxy TCP port.

Example

```
no port
```

Syntax

bypass-upon-failure

Mode

Web Proxy

Description

Enable bypass proxy servers upon proxy server failure.

Example

bypass-upon-failure

Syntax

no bypass-upon-failure

Mode

Web Proxy

Description

Disable bypass proxy servers upon proxy server failure.

Example

no bypass-upon-failure

Syntax

forward-public-requests

Mode

Web Proxy

Description

Enable forward public zone client requests to proxy server.

Example

forward-public-requests

Syntax

no forward-public-requests

Mode

Web Proxy

Description

Disable forward public zone client requests to proxy server.

Example

no forward-public-requests

Syntax

user-proxy-server <WORD>

Mode

Web Proxy

Description

Add proxy server through which users' web requests may come.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-proxy-server example.com
```

Syntax

```
no user-proxy-server <USER_NETPROXY_SERVER>
```

Mode

Web Proxy

Description

Delete proxy server through which users' web requests may come.

Options

<USER_NETPROXY_SERVER> User net proxy server.
Example: *abc*

Example

```
no user-proxy-server example.com
```

Syntax

```
no user-proxy-servers
```

Mode

Web Proxy

Description

Delete all proxy servers through which users' web requests may come.

Example

```
no user-proxy-servers
```

Syntax

```
amazon-web-services connection
```

Mode

Config

Description

Configure Amazon web services connection and enter configuration mode.

Example

```
amazon-web-services connection
```

Syntax

access-key-id <WORD>

Mode

Amazon Web Services

Description

Set Amazon web services access key id.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

access-key-id *AFGRTSRWCGDFTYT4TBQ*

Syntax

no access-key-id

Mode

Amazon Web Services

Description

Clear Amazon web services access key id.

Example

no access-key-id

Syntax

secret <ENC_PASSWORD>

Mode

Amazon Web Services

Description

Set Amazon web services secret access key and confirm.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

secret *ACBYSDTTC7ENTOTTF*

Syntax

no secret

Mode

Amazon Web Services

Description

Clear Amazon web services access key secret and confirmation.

Example

no secret

Syntax

region { canada | frankfurt | ireland | london | mumbai | north-california | north-virginia | ohio | oregon | paris | sao-paulo | seoul | singapore | sydney | tokyo }

Mode

Amazon Web Services

Description

Set Amazon web services region.

Options

<i>canada</i>	Canada (Central).
<i>frankfurt</i>	EU (Frankfurt).
<i>ireland</i>	EU (Ireland).
<i>london</i>	EU (London).
<i>mumbai</i>	Asia Pacific (Mumbai).
<i>north-california</i>	US West (N. California).
<i>north-virginia</i>	US East (N. Virginia).
<i>ohio</i>	US East (Ohio).
<i>oregon</i>	US West (Oregon).
<i>paris</i>	EU (Paris).
<i>sao-paulo</i>	South America (SÃ£o Paulo).
<i>seoul</i>	Asia Pacific (Seoul).
<i>singapore</i>	Asia Pacific (Singapore).
<i>sydney</i>	Asia Pacific (Sydney).
<i>tokyo</i>	Asia Pacific (Tokyo).

Example

region london

Syntax

connect

Mode

Amazon Web Services

Description

Connect Amazon web services using configured parameters.

Example

```
connect
```

Syntax

```
test
```

Mode

Amazon Web Services

Description

Test Amazon web services using configured parameters.

Example

```
test
```

Syntax

```
amazon-web-services objects
```

Mode

Config

Description

Enter Amazon web services objects configuration mode.

Example

```
amazon-web-services objects
```

Syntax

```
mapping
```

Mode

Amazon Web Services Objects

Description

Enable Amazon web services address object mapping.

Example

```
mapping
```

Syntax

```
no mapping
```

Mode

Amazon Web Services Objects

Description

Disable Amazon web services address object mapping.

Example

Syntax

`synchronization-interval <UINT16>`

Mode

Amazon Web Services Objects

Description

Set Amazon web services objects synchronization interval (secs).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: `123`

Example

`synchronization-interval 60`

Syntax

`monitor-region { canada | frankfurt | ireland | london | mumbai | north-california | north-virginia | ohio | oregon | paris | sao-paulo | seoul | singapore | sydney | tokyo }`

Mode

Amazon Web Services Objects

Description

Enable Amazon web services object region to monitor.

Options

canada	Canada (Central).
frankfurt	EU (Frankfurt).
ireland	EU (Ireland).
london	EU (London).
mumbai	Asia Pacific (Mumbai).
north-california	US West (N. California).
north-virginia	US East (N. Virginia).
ohio	US East (Ohio).
oregon	US West (Oregon).
paris	EU (Paris).
sao-paulo	South America (SÃ£o Paulo).
seoul	Asia Pacific (Seoul).
singapore	Asia Pacific (Singapore).
sydney	Asia Pacific (Sydney).
tokyo	Asia Pacific (Tokyo).

Example

```
monitor-region london
```

Syntax

```
no monitor-region { canada | frankfurt | ireland | london | mumbai | north-california | north-virginia | ohio | oregon | paris | sao-paulo | seoul | singapore | sydney | tokyo }
```

Mode

Amazon Web Services Objects

Description

Disable Amazon web services object region to monitor.

Options

<i>canada</i>	Canada (Central).
<i>frankfurt</i>	EU (Frankfurt).
<i>ireland</i>	EU (Ireland).
<i>london</i>	EU (London).
<i>mumbai</i>	Asia Pacific (Mumbai).
<i>north-california</i>	US West (N. California).
<i>north-virginia</i>	US East (N. Virginia).
<i>ohio</i>	US East (Ohio).
<i>oregon</i>	US West (Oregon).
<i>paris</i>	EU (Paris).
<i>sao-paulo</i>	South America (SÃ£o Paulo).
<i>seoul</i>	Asia Pacific (Seoul).
<i>singapore</i>	Asia Pacific (Singapore).
<i>sydney</i>	Asia Pacific (Sydney).
<i>tokyo</i>	Asia Pacific (Tokyo).

Example

```
no monitor-region london
```

Syntax

```
no address-objects
```

Mode

Amazon Web Services Objects

Description

Delete all Amazon web services related address objects and groups.

Example

no address-objects

Syntax

group-mapping <AWS_GROUP_MAPPING_INDEX>

Mode

Amazon Web Services Objects

Description

Add or Edit an aws address group mapping.

Options

<AWS_GROUP_MAPPING_INDEX> Integer in the form: D OR 0xHHHHHHHH.
Example: *1*

Example

group-mapping 1

Syntax

no group-mapping <AWS_GROUP_MAPPING_INDEX>

Mode

Amazon Web Services Objects

Description

Delete an aws address group mapping.

Options

<AWS_GROUP_MAPPING_INDEX> Integer in the form: D OR 0xHHHHHHHH.
Example: *1*

Example

no group-mapping 1

Syntax

no group-mappings

Mode

Amazon Web Services Objects

Description

Delete all aws address group mappings.

Example

no group-mappings

Syntax

address-group <ADDR_CUSTOM_GROUP_NAME_MIXED>

Mode

AWS Objects Group Mapping

Description

Selete an address group.

Options

<ADDR_CUSTOM_GROUP_NAME_MIXED> Custom group address object name.
Example: *Sales Group*

Example

address-group All\ Interface\ IP

Syntax

condition { custom-key <WORD> | instance-property { architecture | image-id | instance-id | instance-state | instance-type | ip-address | private-dns-name | private-ip-address | subnet-id | vpc-id } } value <WORD>

Mode

AWS Objects Group Mapping

Description

Add Amazon web services objects address group mapping condition.

Options

- custom-key** Custom tag.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- instance-property** Instance property.
- architecture** Architecture.
- image-id** Image ID.
- instance-id** Instance ID.
- instance-state** Instance state.
- instance-type** Instance type.
- ip-address** IP address.
- private-dns-name** Private DNS name.
- private-ip-address** Private IP address.
- subnet-id** Subnet ID.
- vpc-id** VPC ID.
- value** Tag value.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

condition instance-property subnet-id value 255.255.255.248

Syntax

```
no condition { custom-key <WORD> | instance-property { architecture | image-id | instance-id | instance-state | instance-type | ip-address | private-dns-name | private-ip-address | subnet-id | vpc-id } } value <WORD>
```

Mode

AWS Objects Group Mapping

Description

Delete Amazon web services objects address group mapping condition.

Options

custom-key <WORD>	Custom tag. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
instance-property	Instance property.
architecture	Architecture.
image-id	Image ID.
instance-id	Instance ID.
instance-state	Instance state.
instance-type	Instance type.
ip-address	IP address.
private-dns-name	Private DNS name.
private-ip-address	Private IP address.
subnet-id	Subnet ID.
vpc-id	VPC ID.
value <WORD>	Tag value. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
no condition instance-property subnet-id value 255.255.255.248
```

Syntax

```
no conditions
```

Mode

AWS Objects Group Mapping

Description

Delete all conditions.

Example

```
no conditions
```

Syntax

```
no ndp entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE>
```

Mode

Config

Description

Delete an NDP entry.

Options

<NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

<NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

<NDP_INTERFACE> Interface name.
Example: *X0*

Example

```
no ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0
```

Syntax

```
no ndp entries
```

Mode

Config

Description

Delete all NDP entries.

Example

```
no ndp entries
```

Syntax

```
ndp reachable-time <UINT16>
```

Mode

Config

Description

Set neighbor discovery base reachable time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
ndp reachable-time 30
```

Syntax

```
no ndp reachable-time
```

Mode

Config

Description

Clear neighbor discovery base reachable time.

Example

no ndp reachable-time

Syntax

ndp entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE>

Mode

Config

Description

Add/edit an NDP entry.

Options

- <NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b
- <NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD
- <NDP_INTERFACE> Interface name.
Example: X0

Example

ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0

Syntax

ip <NDP_IPV6_HOST>

Mode

Static NDP

Description

Configure static NDP IP.

Options

- <NDP_IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

ip 2001:10:10:10:2D0:02BB:03CC:04DD

Syntax

mac <NDP_MAC>

Mode

Static NDP

Description

Configure static NDP MAC address.

Options

- <NDP_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: 00:0C:F1:56:98:AD

Example

mac 00:01:02:03:04:05

Syntax

```
interface <NDP_INTERFACE>
```

Mode

Static NDP

Description

Configure static NDP interface.

Options

<NDP_INTERFACE> Interface name.
Example: *X0*

Example

```
interface X0
```

Syntax

```
clear ndp cache entries
```

Mode

Config
Top Level

Description

Clear all non-permanent entries.

Example

```
clear ndp cache entries
```

Syntax

```
clear ndp cache entry <NDP_FLUSH_IPV6_HOST> <NDP_FLUSH_IF_NAME>
```

Mode

Config
Top Level

Description

Clear one NDP entry.

Options

<NDP_FLUSH_IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

<NDP_FLUSH_IF_NAME> Interface name.
Example: *X0*

Example

```
clear ndp cache entry 2001:10:10:10:2D0:02BB:03CC:04DD X0
```

Syntax

```
tunnel-interface ipv6 <IPV6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Add/edit tunnel interface.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

```
tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
no tunnel-interface ipv6 <IPV6_TUNNEL_INTERFACE>
```

Mode

Config

Description

Delete IPv6 tunnel interface.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

```
no tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
no tunnel-interfaces ipv6
```

Mode

Config

Description

Delete all IPv6 tunnel interface.

Example

```
no tunnel-interfaces ipv6
```

Syntax

```
name <IPV6_TUNNEL_INTERFACE>
```

Mode

Tunnel Interface

Description

Set tunnel interface name.

Options

<IPV6_TUNNEL_INTERFACE> IPv6 Interface name.
Example: *myTunnelInterface*

Example

name CorpIPv6Tunnel

Syntax

zone <INTERFACE_ZONE_NAME>

Mode

Tunnel Interface

Description

Set tunnel interface zone.

Options

<INTERFACE_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

zone WAN

Syntax

no zone

Mode

Tunnel Interface

Description

Clear tunnel interface zone.

Example

no zone

Syntax

type { 6rd | 6to4 | gre | isatap | manual }

Mode

Tunnel Interface

Description

Set the tunnel interface type.

Options

- 6rd** 6rd tunnel.
- 6to4** IPv6 6to4 tunnel.
- gre** GRE tunnel.
- isatap** ISATAP tunnel.
- manual** Manual tunnel.

Example

Syntax

ip <IPv6_HOST>

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Set tunnel interface IPv6 address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

ip 3ffe:1900:4545::f8ff:fe21:67cf

Syntax

no ip

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Clear tunnel interface IPv6 address.

Example

no ip

Syntax

prefix-length <UINT8>

Mode

Manual Tunnel Interface
GRE Tunnel Interface
6to4 Tunnel Interface
6rd Tunnel Interface

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

prefix-length 64

Syntax

comment <WORD>

Mode

Tunnel Interface

Description

Set tunnel interface comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "IPv6 tunnel to Corporate"
```

Syntax

no comment

Mode

Tunnel Interface

Description

Clear tunnel interface comment.

Example

```
no comment
```

Syntax

management { http | https | ping | snmp | ssh }

Mode

Interface IPv6
Tunnel Interface

Description

Enable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
management https
```

Syntax

```
no management { http | https | ping | snmp | ssh }
```

Mode

Interface IPv6
Tunnel Interface

Description

Disable management for the specified protocols.

Options

http HTTP.

https HTTPS.

ping Ping.

snmp SNMP.

ssh SSH.

Example

```
no management https
```

Syntax

```
user-login [ http ] [ https ]
```

Mode

Interface IPv6
Tunnel Interface

Description

Enable user login for the specified protocols.

Options

http HTTP.

https HTTPS.

Example

```
user-login http https
```

Syntax

```
no user-login [ http ] [ https ]
```

Mode

Interface IPv6
Tunnel Interface

Description

Disable user login for the specified protocols.

Options

http HTTP.

https HTTPS.

Example

```
no user-login http
```

Syntax

https-redirect

Mode

Interface IPv6
Tunnel Interface

Description

Enable redirection from HTTP to HTTPS.

Example

https-redirect

Syntax

no https-redirect

Mode

Interface IPv6
Tunnel Interface

Description

Disable redirection from HTTP to HTTPS.

Example

no https-redirect

Syntax

remote ipv4-address { host <TUNNEL_IPV4_ADDR_HOST> | name <TUNNEL_IPV4_ADDR_HOST_NAME> }

Mode

Manual Tunnel Interface

Description

Configure the remote IPv4 address.

Options

host	Configure the remote IPv4 address to host address.
<TUNNEL_IPV4_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Configure the remote IPv4 address to named address object.
<TUNNEL_IPV4_ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>

Example

remote ipv4-address host 198.165.165.4

Syntax

no remote ipv4-address

Mode

Manual Tunnel Interface

Description

Clear the remote IPv4 address.

Example

```
no remote ipv4-address
```

Syntax

```
remote ipv6-network { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

Manual Tunnel Interface

Description

Configure the remote IPv6 network.

Options

group <ADDR_GROUP_NAME>	Configure the remote IPv6 network to named address object group. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Configure the remote network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name <ADDR_NAME>	Configure the remote IPv6 network to named address object. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Configure the remote network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Configure the remote network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>

Example

```
remote ipv6-network name IPv6RemoteNetwork
```

Syntax

```
no remote ipv6-network
```

Mode

Manual Tunnel Interface

Description

Clear the remote IPv6 network.

Example

```
no remote ipv6-network
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

Manual Tunnel Interface

Description

Set tunnel interface bound to.

Options

any	Bound to any interface.
interface <IPV6_TUNNEL_BOUND_TO_INTERFACE>	Bound to interface. Interface name. Example: <i>X0</i>

Example

```
bound-to interface X1
```

Syntax

```
link-mtu <UINT16>
```

Mode

Manual Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
link-mtu 1500
```

Syntax

```
remote ipv4-address { host <TUNNEL_IPV4_ADDR_HOST> | name <TUNNEL_IPV4_ADDR_HOST_NAME> }
```

Mode

GRE Tunnel Interface

Description

Configure the remote IPv4 address.

Options

host <TUNNEL_IPV4_ADDR_HOST>	Configure the remote IPv4 address to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>

name Configure the remote IPv4 address to named address object.
<TUNNEL_IPv4_ADDR_HOST_NAME> Host address object name.
Example: *Web Server*

Example

```
remote ipv4-address host 198.165.165.4
```

Syntax

```
no remote ipv4-address
```

Mode

GRE Tunnel Interface

Description

Clear the remote IPv4 address.

Example

```
no remote ipv4-address
```

Syntax

```
remote ipv6-network { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

GRE Tunnel Interface

Description

Configure the remote IPv6 network.

Options

group Configure the remote IPv6 network to named address object group.
<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Configure the remote network to host address.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

name Configure the remote IPv6 network to named address object.
<ADDR_NAME> Address object name.
Example: *Web Server*

network Configure the remote network to network address.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.
Example: *IPv4: 255.255.255.0\nIPv6: /64\n*

range Configure the remote network to range of addresses.
<ADDR_BEGIN> IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

<ADDR_END> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n*

Example

```
remote ipv6-network name IPv6RemoteNetwork
```

Syntax

```
no remote ipv6-network
```

Mode

GRE Tunnel Interface

Description

Clear the remote IPv6 network.

Example

```
no remote ipv6-network
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

GRE Tunnel Interface

Description

Set tunnel interface bound to.

Options

<i>any</i>	Bound to any interface.

<i>interface</i>	Bound to interface.

<i><IPV6_TUNNEL_BOUND_TO_INTERFACE></i>	Interface name. Example: <i>X0</i>

Example

```
bound-to interface X1
```

Syntax

```
link-mtu <UINT16>
```

Mode

GRE Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
link-mtu 1500
```

Syntax

```
bound-to { any | interface <IPV6_TUNNEL_BOUND_TO_INTERFACE> }
```

Mode

6to4 Tunnel Interface

Description

Set 6to4 tunnel interface bound to.

Options

any	Bound to any interface.
interface	Bound to interface.
<IPV6_TUNNEL_BOUND_TO_INTERFACE>	Interface name. Example: <i>X0</i>

Example

```
bound-to interface X1
```

Syntax

```
enable
```

Mode

6to4 Tunnel Interface

Description

Enable IPv6 6to4 tunnel.

Example

```
enable
```

Syntax

```
no enable
```

Mode

6to4 Tunnel Interface

Description

Disable IPv6 6to4 tunnel.

Example

```
no enable
```

Syntax

```
link-mtu <UINT16>
```

Mode

6to4 Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

link-mtu 1500

Syntax

bound-to interface <IPV6_TUNNEL_BOUND_TO_INTERFACE>

Mode

6rd Tunnel Interface

Description

Set tunnel interface bound to.

Options

<i>interface</i>	Bound to interface.
<i><IPV6_TUNNEL_BOUND_TO_INTERFACE></i>	Interface name. Example: X0

Example

bound-to interface X1

Syntax

no bound-to

Mode

6rd Tunnel Interface

Description

Clear tunnel interface bound to.

Example

no bound-to

Syntax

dynamic

Mode

6rd Tunnel Interface

Description

Enable dynamic acquisition of IP configuration data.

Example

dynamic

Syntax

no dynamic

Mode

6rd Tunnel Interface

Description

Disable dynamic acquisition of IP configuration data.

Example

```
no dynamic
```

Syntax

```
6rd prefix <IPv6_HOST>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface 6rd prefix.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
6rd prefix 2001::
```

Syntax

```
no 6rd prefix
```

Mode

6rd Tunnel Interface

Description

Clear tunnel interface 6rd prefix.

Example

```
no 6rd prefix
```

Syntax

```
6rd prefix-length <UINT8>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface 6rd prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
6rd prefix-length 64
```

Syntax

no 6rd prefix-length

Mode

6rd Tunnel Interface

Description

Clear tunnel interface 6rd prefix length.

Example

no 6rd prefix-length

Syntax

border-relay-ipv4-address <IPV4_HOST>

Mode

6rd Tunnel Interface

Description

Set tunnel interface border relay IPv4 address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

border-relay-ipv4-address 10.10.10.10

Syntax

no border-relay-ipv4-address

Mode

6rd Tunnel Interface

Description

Clear tunnel interface border relay IPv4 address.

Example

no border-relay-ipv4-address

Syntax

mask-length <UINT8>

Mode

6rd Tunnel Interface

Description

Set tunnel interface IPv4 mask length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
mask-length 64
```

Syntax

```
no mask-length
```

Mode

6rd Tunnel Interface

Description

Clear tunnel interface IPv4 mask length.

Example

```
no mask-length
```

Syntax

```
link-mtu <UINT16>
```

Mode

6rd Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
link-mtu 1500
```

Syntax

```
default-route
```

Mode

6rd Tunnel Interface

Description

Enable add default route.

Example

```
default-route
```

Syntax

```
no default-route
```

Mode

6rd Tunnel Interface

Description

Disable add default route.

Example

no default-route

Syntax

bound-to interface <IPV6_TUNNEL_BOUND_TO_INTERFACE>

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface bound to.

Options

interface Bound to interface.
<IPV6_TUNNEL_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

Example

bound-to interface X1

Syntax

no bound-to

Mode

ISATAP Tunnel Interface

Description

Clear tunnel interface bound to.

Example

no bound-to

Syntax

prefix { name <ISATAP_ADDR_NETWORK_NAME> | network <ISATAP_ADDR_NETWORK> <ISATAP_ADDR_MASK> }

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface IPv6 subnet prefix.

Options

name Set tunnel interface IPv6 subnet prefix to named address object.
<ISATAP_ADDR_NETWORK_NAME> Network address object name.
Example: *Sales Network*

network Set tunnel interface IPv6 subnet prefix to network address.
<ISATAP_ADDR_NETWORK> IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*
<ISATAP_ADDR_MASK> IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n.
Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

Example

```
prefix name ipv6Network
```

Syntax

```
no prefix
```

Mode

ISATAP Tunnel Interface

Description

Clear tunnel interface IPv6 subnet prefix.

Example

```
no prefix
```

Syntax

```
link-mtu <UINT16>
```

Mode

ISATAP Tunnel Interface

Description

Set tunnel interface link MTU.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
link-mtu 1500
```

Syntax

```
ipv6-traffic
```

Mode

Interface IPv6

Description

Enable IPv6 traffic on this interface.

Example

```
ipv6-traffic
```

Syntax

```
no ipv6-traffic
```

Mode

Interface IPv6

Description

Disable IPv6 traffic on this interface.

Example

```
no ipv6-traffic
```

Syntax

```
listen-router-advertisement
```

Mode

Interface IPv6

Description

Enable listening to route advertisement.

Example

```
listen-router-advertisement
```

Syntax

```
no listen-router-advertisement
```

Mode

Interface IPv6

Description

Disable listening to route advertisement.

Example

```
no listen-router-advertisement
```

Syntax

```
stateless-address-autoconfig
```

Mode

Interface IPv6

Description

Enable stateless address autoconfiguration.

Example

```
stateless-address-autoconfig
```

Syntax

```
no stateless-address-autoconfig
```

Mode

Interface IPv6

Description

Disable stateless address autoconfiguration.

Example

no stateless-address-autoconfig

Syntax

duplicate-address-detection-transmits <UINT8>

Mode

Interface IPv6

Description

Set duplicate address detection transmits.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

duplicate-address-detection-transmits 1

Syntax

no duplicate-address-detection-transmits

Mode

Interface IPv6

Description

Clear duplicate address detection transmits.

Example

no duplicate-address-detection-transmits

Syntax

reachable-time <UINT16>

Mode

Interface IPv6

Description

Set neighbor discovery base reachable time in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

reachable-time 30

Syntax

no reachable-time

Mode

Interface IPv6

Description

Clear neighbor discovery base reachable time.

Example

```
no reachable-time
```

Syntax

```
ip-assignment [ mode ] { auto | dhcpv6 | l2bridge | pppoe6 | static }
```

Mode

Interface IPv6

Description

Set interface IPv6 assignment.

Options

mode	Interface IP assignment mode.
auto	Interface IPv6 configuration set to auto.
dhcpv6	Interface IPv6 configuration obtained by dhcpv6.
l2bridge	Interface uses layer two bridging.
pppoe6	PPPoE IPv6 configuration assignment.
static	Static IPv6 configuration assignment.

Example

```
ip-assignment dhcpv6
ip-assignment static
ip-assignment auto
ip-assignment pppoe6
```

Syntax

```
no ip-assignment
```

Mode

Interface IPv6

Description

Clear interface IPv6 assignment.

Example

```
no ip-assignment
```

Syntax

```
ip <IPV6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface IPv6 address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
no ip
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear interface IPv6 address.

Example

```
no ip
```

Syntax

```
prefix-length <UINT8>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
prefix-length 64
```

Syntax

```
dns primary <IPV6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the primary DNS server IP address.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
dns primary 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
dns secondary <IPv6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the secondary DNS server IP address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
dns secondary 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
dns tertiary <IPv6_HOST>
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set the tertiary DNS server IP address.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

```
dns tertiary 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
no dns primary
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the primary DNS server IP address.

Example

```
no dns primary
```

Syntax

no dns secondary

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the secondary DNS server IP address.

Example

no dns secondary

Syntax

no dns tertiary

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear the tertiary DNS server IP address.

Example

no dns tertiary

Syntax

gateway <IPv6_HOST>

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Set interface gateway.

Options

<IPv6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

gateway 3ffe:1900:4545:201::202

Syntax

no gateway

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Clear interface gateway.

Example

no gateway

Syntax

advertise-subnet-prefix

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Enable advertise subnet prefix of IPv6 primary static address.

Example

advertise-subnet-prefix

Syntax

no advertise-subnet-prefix

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Disable advertise subnet prefix of IPv6 primary static address.

Example

no advertise-subnet-prefix

Syntax

extra-ip [type] { 6rd <IPv6_EXTRA_ADDR> | prefix-delegation <IPv6_EXTRA_ADDR> | static <IPv6_EXTRA_ADDR> }

Mode

Static IPv6 Assignment

Description

Add/edit extra interface IPv6 address.

Options

<i>type</i>	Type
<i>6rd</i>	Add downstream IPv6 address delegated from 6rd
<i><IPv6_EXTRA_ADDR></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>prefix-delegation</i>	Add downstream IPv6 address delegated from DHCP-PD
<i><IPv6_EXTRA_ADDR></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>static</i>	Add static IPv6 address
<i><IPv6_EXTRA_ADDR></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

extra-ip static 3ffe:1900:4545::f8ff:fe21:67c2

Syntax

```
no extra-ip [ type ] { 6rd | prefix-delegation | static } <IPv6_EXTRA_ADDR>
```

Mode

Static IPv6 Assignment

Description

Delete extra interface IPv6 address.

Options

<i>type</i>	Type
<i>6rd</i>	Delete downstream IPv6 address delegated from 6rd
<i>prefix-delegation</i>	Delete downstream IPv6 address delegated from DHCP-PD
<i>static</i>	Delete statioc IPv6 address
<i><IPv6_EXTRA_ADDR></i>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
no extra-ip static 3ffe:1900:4545::f8ff:fe21:67c2
```

Syntax

```
no extra-ipv6-addresses
```

Mode

Static IPv6 Assignment

Description

Delete all extra interface IPv6 addresses.

Example

```
no extra-ipv6-addresses
```

Syntax

```
router-advertisement
```

Mode

Static IPv6 Assignment
PPPoEv6 Assignment

Description

Enter router advertisement configuration mode.

Example

```
router-advertisement
```

Syntax

```
one-arm-mode
```

Mode

Interface IPv6

Description

Enable interface one-arm mode.

Example

```
one-arm-mode
```

Syntax

```
no one-arm-mode
```

Mode

Interface IPv6

Description

Disable interface one-arm mode.

Example

```
no one-arm-mode
```

Syntax

```
one-arm-peer <IPV6_HOST>
```

Mode

Interface IPv6

Description

Set interface one-arm peer.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
one-arm-peer 100::1
```

Syntax

```
no one-arm-peer
```

Mode

Interface IPv6

Description

Disable interface one-arm peer.

Example

```
no one-arm-peer
```

Syntax

```
multicast
```

Mode

Interface IPv6

Description

Enable IPv6 multicast support.

Example

multicast

Syntax

no multicast

Mode

Interface IPv6

Description

Disable IPv6 multicast support.

Example

no multicast

Syntax

type { 6rd | prefix-delegation | static }

Mode

IPv6 Extra Address

Description

Set interface IPv6 extra address type.

Options

- 6rd** Add downstream IPv6 address delegated from 6rd
- prefix-delegation** Add downstream IPv6 address delegated from DHCP-PD
- static** Add statioc IPv6 address

Example

type static

Syntax

ip <IPV6_EXTRA_ADDR>

Mode

IPv6 Extra Address

Description

Set interface IPv6 address.

Options

- <IPV6_EXTRA_ADDR>** IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
ip 3ffe:1900:4545::f8ff:fe21:67cf
```

Syntax

```
prefix-length <UINT8>
```

Mode

IPv6 Extra Address

Description

Set interface IPv6 prefix length.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
prefix-length 64
```

Syntax

```
delegated-prefix <DELEGATED_PREFIX_ADDR_HOST_NAME>
```

Mode

IPv6 Extra Address

Description

Set delegated prefix assignment.

Options

<DELEGATED_PREFIX_ADDR_HOST_NAME> Host address object name.
Example: Web Server

Example

```
delegated-prefix "X3 Delegated Prefix"
```

Syntax

```
no delegated-prefix
```

Mode

IPv6 Extra Address

Description

Clear delegated prefix assignment.

Example

```
no delegated-prefix
```

Syntax

```
preferred-ip <IPV6_EXTRA_ADDR>
```

Mode
IPv6 Extra Address
Description
Set interface preferred IPv6 address.
Options
<IPv6_EXTRA_ADDR> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b
Example
<i>preferred-ip 3ffe:1900:4545::f8ff:fe21:67cf</i>

Syntax
<i>preferred-prefix-length <UINT8></i>
Mode
IPv6 Extra Address
Description
Set interface IPv6 preferred prefix length.
Options
<UINT8> Integer in the form: D OR 0xHH. Example: 123
Example
<i>preferred-prefix-length 64</i>

Syntax
<i>no preferred-prefix-length</i>
Mode
IPv6 Extra Address
Description
Clear interface IPv6 preferred prefix length.
Example
<i>no preferred-prefix-length</i>

Syntax
<i>advertise-subnet-prefix</i>
Mode
IPv6 Extra Address
Description
Enable advertise subnet prefix of IPv6 address.
Example
<i>advertise-subnet-prefix</i>

Syntax

no advertise-subnet-prefix

Mode

IPv6 Extra Address

Description

Disable advertise subnet prefix of IPv6 address.

Example

no advertise-subnet-prefix

Syntax

enable

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable IPv6 router advertisement.

Example

enable

Syntax

no enable

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable IPv6 router advertisement.

Example

no enable

Syntax

interval { max <UINT32> | min <UINT32> }

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement interval range.

Options

max	Router advertisement interval range maximum.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

min Router advertisement interval range minimum.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

interval min 200

Syntax

link-mtu <UINT32>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement link MTU.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

link-mtu 1400

Syntax

no link-mtu

Mode

Static IPv6 Assignment Router Advertisement

Description

Set IPv6 router advertisement link MTU as unspecified.

Example

no link-mtu

Syntax

reachable-time <UINT32>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set the time the node assumes the neighbor is reachable in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

reachable-time 5

Syntax

no reachable-time

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the time the node assumes the neighbor is reachable as unspecified.

Example

no reachable-time

Syntax

retransmit-timer <UINT32>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set the time between retransmitted neighbor solicitation messages in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

retransmit-timer 30

Syntax

no retransmit-timer

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the time between retransmitted neighbor solicitation messages as unspecified.

Example

no retransmit-timer

Syntax

current-hop-limit <UINT8>

Mode

Static IPv6 Assignment Router Advertisement

Description

Set current hop limit.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
current-hop-limit 64
```

Syntax

```
no current-hop-limit
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Set current hop limit as unspecified.

Example

```
no current-hop-limit
```

Syntax

```
router lifetime <UINT16>
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Configure the lifetime when a router is accepted as the default router in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
router lifetime 1800
```

Syntax

```
no router lifetime
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Clear the lifetime when a router is accepted as the default router as unspecified.

Example

```
no router lifetime
```

Syntax

```
router preference { high | low | medium }
```

Mode

Static IPv6 Assignment Router Advertisement

Description

Configure router preference when a router is accepted as the default router.

Options

high Set the router preference as high.

low Set the router preference as low.

medium Set the router preference as medium.

Example

```
router preference low
```

Syntax

managed

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable IPv6 addresses as available via stateful addresses configuration.

Example

managed

Syntax

no managed

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable IPv6 addresses as available via stateful addresses configuration.

Example

no managed

Syntax

other-config

Mode

Static IPv6 Assignment Router Advertisement

Description

Enable non-address configuration as available via stateful addresses configuration.

Example

other-config

Syntax

no other-config

Mode

Static IPv6 Assignment Router Advertisement

Description

Disable non-address configuration as available via stateful addresses configuration.

Example

no other-config

Syntax

prefix <IPv6_ADVERTISING_PREFIX>

Mode

Static IPv6 Assignment Router Advertisement

Description

Add/edit advertising prefix.

Options

<IPv6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2001::*

Example

prefix 2001:1:1:1::

Syntax

no prefix <IPv6_ADVERTISING_PREFIX>

Mode

Static IPv6 Assignment Router Advertisement

Description

Delete the specified advertising prefix.

Options

<IPv6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2001::*

Example

no prefix 2001:1:1:1::

Syntax

no prefixes

Mode

Static IPv6 Assignment Router Advertisement

Description

Delete all advertising prefixes.

Example

no prefixes

Syntax

prefix <IPv6_ADVERTISING_PREFIX>

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Set advertising prefix.

Options

<IPv6_ADVERTISING_PREFIX> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2001::*

Example

prefix 2001:1:1:1::

Syntax

valid-lifetime <UINT32>

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Set advertising prefix valid lifetime in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

valid-lifetime 10

Syntax

no valid-lifetime

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Clear advertising prefix valid lifetime in minutes.

Example

no valid-lifetime

Syntax

preferred lifetime <UINT32>

Mode

Description

Set advertising prefix valid preferred lifetime in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
preferred lifetime 10
```

Syntax

```
no preferred lifetime
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Clear advertising prefix valid preferred lifetime in minutes.

Example

```
no preferred lifetime
```

Syntax

```
on-link
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Enable using prefix for on-link determination.

Example

```
on-link
```

Syntax

```
no on-link
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Disable using prefix for on-link determination.

Example

```
no on-link
```

Syntax

```
autonomous
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Enable autonomous address configuration indicating prefix can be used for stateless address configuration.

Example

```
autonomous
```

Syntax

```
no autonomous
```

Mode

Static IPv6 Assignment Router Advertisement Prefix

Description

Disable autonomous address configuration.

Example

```
no autonomous
```

Syntax

```
prefix-delegation
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable DHCPv6 prefix delegation.

Example

```
prefix-delegation
```

Syntax

```
no prefix-delegation
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable DHCPv6 prefix delegation.

Example

```
no prefix-delegation
```

Syntax

```
rapid-commit
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Enable use rapid commit option.

Example

```
rapid-commit
```

Syntax

```
no rapid-commit
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Disable use rapid commit option.

Example

```
no rapid-commit
```

Syntax

```
aftr-name-option
```

Mode

DHCPv6 Assignment

Description

Enable use AFTR (Address Family Transition Router) name option.

Example

```
aftr-name-option
```

Syntax

```
no aftr-name-option
```

Mode

DHCPv6 Assignment

Description

Disable use AFTR (Address Family Transition Router) name option.

Example

```
no aftr-name-option
```

Syntax

```
release [ delegated-prefix ]
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Release designated interface lease or delegated prefixes acquired via DHCPv6.

Options

delegated-prefix Release delegated prefixes acquired via DHCPv6.

Example

```
release
```

Syntax

```
renew [ delegated-prefix ]
```

Mode

DHCPv6 Assignment
PPPoEv6 Assignment

Description

Renew designated interface lease or delegated prefixes acquired via DHCPv6.

Options

delegated-prefix Renew delegated prefixes acquired via DHCPv6.

Example

```
renew
```

Syntax

```
mode-assignment { auto | dhcpv6 | static }
```

Mode

PPPoEv6 Assignment

Description

Set PPPoE IPv6 address mode.

Options

auto Set PPPoE6 to auto mode.

dhcpv6 Set PPPoE6 to dhcpv6 mode.

static Set PPPoE6 to static mode.

Example

```
mode-assignment dhcpv6
mode-assignment static
mode-assignment auto
```

Syntax

```
ncp-neg-retrans <UINT16>
```

Mode

Description

Set the NCP retransmission time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

ncp-neg-retrans 200

Syntax

schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

Description

Set the wan pppoe reconnect schedule.

Options

always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "Work Hours"

Syntax

inactivity <UINT16>

Mode

Description

Enable the pppoe inactivity timer.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

inactivity 10

Syntax

no inactivity

Mode

PPPoEv6 Assignment

Description

Disable the pppoe inactivity timer.

Example

no inactivity

Syntax

lcp-echo-packets

Mode

PPPoEv6 Assignment

Description

Enable strictly use LCP echo packets for server keep-alive.

Example

lcp-echo-packets

Syntax

no lcp-echo-packets

Mode

PPPoEv6 Assignment

Description

Disable strictly use LCP echo packets for server keep-alive.

Example

no lcp-echo-packets

Syntax

reconnect <UINT16>

Mode

PPPoEv6 Assignment

Description

Enable and set reconnect the PPPOE client if the server does not send traffic for specified minutes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

reconnect 5

Syntax

no reconnect

Mode

PPPoEv6 Assignment

Description

Disable reconnect the PPPOE client if the server does not send traffic.

Example

no reconnect

Syntax

enable

Mode

IPv6 DHCP Server

Description

Enable IPv6 DHCP server.

Example

enable

Syntax

no enable

Mode

IPv6 DHCP Server

Description

Disable IPv6 DHCP server.

Example

no enable

Syntax

option object <DHCP_OPTION_OBJECT>

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

option object "LAN Specific DHCP Option"

Syntax

```
no option object <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server option object.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
no option object "LAN Specific DHCP Option"
```

Syntax

```
no option objects
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server option objects.

Example

```
no option objects
```

Syntax

```
name <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object name.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
name "LAN Specific DHCP Option"
```

Syntax

```
number <DHCP_IPV6_OPTION_OBJECT_NUMBER>
```

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object number.

Options

<DHCP_IPV6_OPTION_OBJECT_NUMBER> IPv6 DHCP server option object number.
Example: *12*

Example

number 12

Syntax

array

Mode

IPv6 DHCP Option Object

Description

Enable IPv6 DHCP server option object array.

Example

array

Syntax

no array

Mode

IPv6 DHCP Option Object

Description

Disable IPv6 DHCP server option object array.

Example

no array

Syntax

value { boolean <UINT8> | domain-name <HOSTNAME> | four-byte <UINT32> | ip <IPV6_HOST> | one-byte <UINT8> | string <WORD> | two-byte <UINT16> }

Mode

IPv6 DHCP Option Object

Description

Set IPv6 DHCP server option object value. If Option Array is checked , multiple values can be entered separated by ;.

Options

- boolean**

Option object type: boolean.
- <UINT8>**

Integer in the form: D OR 0xHH.
Example: *123*
- domain-name**

Option object type: domain name.
- <HOSTNAME>**

Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
- four-byte**

Option object type: four byte data.
- <UINT32>**

Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

ip	Option object type: IP address.
<IPv6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
one-byte	Option object type: one byte.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
string	Option object type: string.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
two-byte	Option object type: two byte.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
value ip fe80::1
value domain-name domainName
value four-byte 123
value two-byte 123
value one-byte 23
value string "String value"
value boolean 0
```

Syntax

```
no value
```

Mode

IPv6 DHCP Option Object

Description

Clear IPv6 DHCP server option object value.

Example

```
no value
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server option group.

Options

```
<DHCP_OPTION_GROUP> DHCP server option group name.
                        Example: Corp Network DHCP Group
```

Example

```
option group "LAN Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP>
```

Mode

Description

Delete one IPv6 DHCP server option group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
no option group "LAN Specific DHCP Options"
```

Syntax

```
no option groups
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server option groups.

Example

```
no option groups
```

Syntax

```
name <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Set IPv6 DHCP server option group name.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
name "LAN Specific DHCP Options"
```

Syntax

```
option object <DHCP_OPTION_OBJECT>
```

Mode

IPv6 DHCP Server Option Group

Description

Add IPv6 DHCP server option object to group.

Options

<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
option object "Specific DHCP Options"
```

Syntax

```
no option object <DHCP_OPTION_GROUP_OBJECT>
```

Mode

IPv6 DHCP Server Option Group

Description

Remove IPv6 DHCP server option object from group.

Options

<DHCP_OPTION_GROUP_OBJECT> DHCP server option object name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option object "Specific DHCP Options"
```

Syntax

```
option group <DHCP_OPTION_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Add IPv6 DHCP server option group to group.

Options

<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*

Example

```
option group "Specific DHCP Options"
```

Syntax

```
no option group <DHCP_OPTION_GROUP_GROUP>
```

Mode

IPv6 DHCP Server Option Group

Description

Remove IPv6 DHCP server option group from group.

Options

<DHCP_OPTION_GROUP_GROUP> DHCP server option group name in specify option group.
Example: *Corp Network DHCP Group*

Example

```
no option group "Specific DHCP Options"
```

Syntax

```
scope dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP dynamic scope and enter its configuration mode.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

```
scope dynamic "dyanmicScope"
```

Syntax

```
no scope dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Delete one IPv6 DHCP dynamic scope.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

```
no scope dynamic "dyanmicScope"
```

Syntax

```
no scopes dynamic
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server dynamic scope.

Example

```
no scopes dynamic
```

Syntax

```
name <DHCP_IPV6_DYNAMIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope name.

Options

<DHCP_IPV6_DYNAMIC_SCOPE_NAME> IPv6 DHCP server dynamic scope name.
Example: *abc*

Example

name "Dynamic Scope Name"

Syntax

enable

Mode

IPv6 DHCP Server Dynamic Scope

Description

Enable IPv6 DHCP server dynamic scope.

Example

enable

Syntax

no enable

Mode

IPv6 DHCP Server Dynamic Scope

Description

Disable IPv6 DHCP server dynamic scope.

Example

no enable

Syntax

prefix <IPv6_HOST>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope prefix.

Options

<IPv6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

prefix fe00::

Syntax

no prefix

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope prefix.

Example

no prefix

Syntax

range <IPV6_HOST> <IPV6_HOST>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP dynamic scope range.

Options

- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

range fe00::1 fe00::2014

Syntax

no range

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP servr dynamic scope range.

Example

no range

Syntax

lifetime valid <UINT32>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope valid lifetime (minutes).

Options

- <UINT32>** Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

lifetime valid 2160

Syntax

no lifetime valid

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope valid lifetime.

Example

no lifetime valid

Syntax

lifetime preferred <UINT32>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope preferred lifetime (minutes).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

lifetime preferred 1440

Syntax

no lifetime preferred

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope preferred lifetime.

Example

no lifetime preferred

Syntax

comment <WORD>

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Comment for dynamic scope"
```

Syntax

```
no comment
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope comment.

Example

```
no comment
```

Syntax

```
always-send-option
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Enable IPv6 DHCP server dynamic scope always send IPv6 options.

Example

```
always-send-option
```

Syntax

```
no always-send-option
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Diablo IPv6 DHCP server dynamic scope always send IPv6 options.

Example

```
no always-send-option
```

Syntax

```
domain-name <HOSTNAME>
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server dynamic scope domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain-name example.com
```

Syntax

```
no domain-name
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope domain name.

Example

```
no domain-name
```

Syntax

```
dns server { inherit | static { primary <IPV6_HOST> | secondary <IPV6_HOST> | tertiary <IPV6_HOST> } }
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

set IPv6 DHCP server DNS settings or inherit DNS settings dynamically from the sonicwall's DNS settings.

Options

inherit Inherit DNS servers.

static Static DNS server.

primary Specify primary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

secondary Specify secondary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

tertiary Specify tertiary DNS server IP address.

<IPV6_HOST> IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
dns server primary fe80::1
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

Description

Clear IPv6 DHCP server dynamic scope DNS server IP.

Options

- static** Clear static IPv6 DHCP server dynamic scope DNS server IP.
- primary** Clear primary DNS server IP address.
- secondary** Clear secondary DNS server IP address.
- tertiary** Clear tertiary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Set IPv6 DHCP server option object or group for dynamic scope.

Options

- group** Set IPv6 DHCP server option group for dynamic scope.
<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*
- object** Set IPv6 DHCP server option object for dynamic scope.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
generic-option object "Specific object DHCP Option" generic-option group "Specific Group DHCP Option"
```

Syntax

```
no generic-option
```

Mode

IPv6 DHCP Server Dynamic Scope

Description

Clear IPv6 DHCP server dynamic scope generic option.

Example

```
no generic-option
```

Syntax

```
scope static <DHCP_IPV6_STATIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Add/edit IPv6 DHCP server static scope.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

```
scope static "dhcps6StaticName"
```

Syntax

```
no scope static <DHCP_IPV6_STATIC_SCOPE_NAME>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server static scope.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

```
no scope static fe00::1
```

Syntax

```
no scopes static
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server static scopes.

Example

```
no scopes static
```

Syntax

```
enable
```

Mode

IPv6 DHCP Server Static Scope

Description

Enable IPv6 DHCP server static scope.

Example

```
enable
```

Syntax

no enable

Mode

IPv6 DHCP Server Static Scope

Description

Disable IPv6 DHCP server static scope.

Example

no enable

Syntax

name <DHCP_IPV6_STATIC_SCOPE_NAME>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope name.

Options

<DHCP_IPV6_STATIC_SCOPE_NAME> IPv6 DHCP server static scope name.
Example: *abc*

Example

name "Static scope Name"

Syntax

no name

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope name.

Example

no name

Syntax

prefix <IPv6_HOST>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope prefix.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

prefix fe00::

Syntax

no prefix

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope prefix.

Example

no prefix

Syntax

ip <IPV6_HOST>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope IP.

Options

<IPV6_HOST> IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: 2000:0000:0000:ff68:0205:62ef:ee8d:f25b

Example

ip fe80::10

Syntax

no ip

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope IP.

Example

no ip

Syntax

iaid <UINT32>

Mode

Description

Set IPv6 DHCP server static scope IAID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
iaid 2014
```

Syntax

```
no iaid
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope IAID.

Example

```
no iaid
```

Syntax

```
duid <WORD>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope DUID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
duid 0003000110F0A0F3A23B
```

Syntax

```
no duid
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope DUID.

Example

```
no duid
```

Syntax

```
lifetime { preferred <UINT32> | valid <UINT32> }
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope valid or preferred lifetime (minutes).

Options

preferred Set IPv6 DHCP server static scope preferred lifetime (minutes).
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

valid Set IPv6 DHCP server static scope valid lifetime (minutes).
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
lifetime valid 2160
lifetime preferred 1440
```

Syntax

```
no lifetime { preferred | valid }
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope valid or preferred lifetime.

Options

preferred Clear IPv6 DHCP server static scope preferred lifetime.

valid Clear IPv6 DHCP server static scope valid lifetime.

Example

```
no lifetime valid
no lifetime preferred
```

Syntax

```
comment <WORD>
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

commnet "IPv6 DHCP server commnet"

Syntax

no comment

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope comment.

Example

no comment

Syntax

always-send-option

Mode

IPv6 DHCP Server Static Scope

Description

Enable send IPv6 DHCP server options always.

Example

always-send-option

Syntax

no always-send-option

Mode

IPv6 DHCP Server Static Scope

Description

Disable send IPv6 DHCP server options always.

Example

no always-send-option

Syntax

domain-name <HOSTNAME>

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server static scope domain name.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
domain-name "IPv6 DHCP server domain name"
```

Syntax

```
no domain-name
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope domain name.

Example

```
no domain-name
```

Syntax

```
dns server { inherit | static { primary <IPv6_HOST> | secondary <IPv6_HOST> | tertiary <IPv6_HOST> } }
```

Mode

IPv6 DHCP Server Static Scope

Description

set IPv6 DHCP server DNS settings or inherit DNS settings dynamically from the SonicWall's DNS settings.

Options

<i>inherit</i>	Inherit DNS servers.
<i>static</i>	Static DNS server.
<i>primary</i> <IPv6_HOST>	Specify primary DNS server IP address. IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>secondary</i> <IPv6_HOST>	Specify secondary DNS server IP address. IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>tertiary</i> <IPv6_HOST>	Specify tertiary DNS server IP address. IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>

Example

```
dns server primary fe80::1  
dns server inherit
```

Syntax

```
no dns server { primary | secondary | tertiary }
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope DNS server IP.

Options

- primary** Clear primary DNS server IP address.
- secondary** Clear secondary DNS server IP address.
- tertiary** Clear tertiary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
generic-option { group <DHCP_OPTION_GROUP> | object <DHCP_OPTION_OBJECT> }
```

Mode

IPv6 DHCP Server Static Scope

Description

Set IPv6 DHCP server option object or group for static scope.

Options

- group** Set IPv6 DHCP server option group for static scope.
<DHCP_OPTION_GROUP> DHCP server option group name.
Example: *Corp Network DHCP Group*
- object** Set IPv6 DHCP server option object for static scope.
<DHCP_OPTION_OBJECT> DHCP server option object name.
Example: *Corp Network DHCP Options*

Example

```
generic-option object "Specific object DHCP Option" generic-option group "Specific Group DHCP Option"
```

Syntax

```
no generic-option
```

Mode

IPv6 DHCP Server Static Scope

Description

Clear IPv6 DHCP server static scope generic option.

Example

```
no generic-option
```

Syntax

```
clear lease <DHCP_IPV6_LEASE_HOST>
```

Mode

IPv6 DHCP Server

Description

Delete IPv6 DHCP server lease.

Options

<DHCP_IPV6_LEASE_HOST> IPv6 DHCP server lease IP.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
clear lease fe80::100
```

Syntax

```
clear leases
```

Mode

IPv6 DHCP Server

Description

Delete all IPv6 DHCP server leases.

Example

```
clear leases
```

Syntax

```
dns-proxy
```

Mode

Config

Description

Configure and enter to DNS proxy mode.

Example

```
dns-proxy
```

Syntax

```
enable
```

Mode

DNS proxy

Description

Enable DNS proxy.

Example

```
enable
```

Syntax

```
no enable
```

Mode

DNS proxy

Description

Disable DNS proxy.

Example

```
no enable
```

Syntax

```
mode { ipv4-to-ipv4 | ipv4-to-ipv6 }
```

Mode

DNS proxy

Description

Set the IP version of sending and receiving DNS proxy packets.

Options

ipv4-to-ipv4 Set IPv4 to IPv4 mode.

ipv4-to-ipv6 Set IPv4 to IPv6 mode.

Example

```
mode ipv4-to-ipv4 mode ipv4-to-ipv6
```

Syntax

```
protocol { udp-only | udp-tcp }
```

Mode

DNS proxy

Description

Set DNS proxy protocol to support DNS resolution over TCP.

Options

udp-only UDP only.

udp-tcp UDP and TCP.

Example

```
protocol udp-tcp protocol udp-only
```

Syntax

```
enforce-all-dns-requests
```

Mode

DNS proxy

Description

Enable enforce DNS proxy for all DNS requests.

Example

```
enforce-all-dns-requests
```

Syntax

no enforce-all-dns-requests

Mode

DNS proxy

Description

Disable enforce DNS proxy for all DNS requests.

Example

no enforce-all-dns-requests

Syntax

dns-cache

Mode

DNS proxy

Description

Enable DNS cache.

Example

dns-cache

Syntax

no dns-cache

Mode

DNS proxy

Description

Disable DNS cache.

Example

no dns-cache

Syntax

no cache-entries

Mode

DNS proxy

Description

Delete all the static DNS cache entries.

Example

no cache-entries

Syntax

```
no cache-entry <DNS_PROXY_STATIC_DNS_CACHE_NAME>
```

Mode

DNS proxy

Description

Delete the specified static DNS cache entry.

Options

<DNS_PROXY_STATIC_DNS_CACHE_NAME> Static DNS cache domain name.
Example: *sonicwall.com*

Example

```
no cache-entry sonicwall.com
```

Syntax

```
cache-entry <DNS_PROXY_STATIC_DNS_CACHE_NAME>
```

Mode

DNS proxy

Description

Add/edit the static DNS cache and enter its configuration mode.

Options

<DNS_PROXY_STATIC_DNS_CACHE_NAME> Static DNS cache domain name.
Example: *sonicwall.com*

Example

```
cache-entry sonicwall.com
```

Syntax

```
domain <DNS_PROXY_STATIC_DNS_CACHE_NAME>
```

Mode

DNS Proxy Static DNS Cache

Description

Set the domain name of the static DNS cache entry.

Options

<DNS_PROXY_STATIC_DNS_CACHE_NAME> Static DNS cache domain name.
Example: *sonicwall.com*

Example

```
domain sonicwall.com
```

Syntax

```
no address ipv4 { primary | secondary }
```

Mode

Description

Clear the static DNS cache entry IPv4 address.

Options

- primary*** Clear the static DNS cache entry primary IPv4 address.
- secondary*** Clear the static DNS cache entry secondary IPv4 address.

Example

```
no address ipv4 primary
no address ipv4 secondary
```

Syntax

```
address ipv4 { primary <IPv4_HOST> | secondary <IPv4_HOST> }
```

Mode

DNS Proxy Static DNS Cache

Description

Set the static DNS cache entry IPv4 address.

Options

- primary*** The primary address
- <IPv4_HOST>*** IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*
- secondary*** The secondary address.
- <IPv4_HOST>*** IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
address ipv4 primary 10.10.10.10
address ipv4 secondary 10.10.10.10
```

Syntax

```
no address ipv6 { primary | secondary }
```

Mode

DNS Proxy Static DNS Cache

Description

Clear the static DNS cache entry IPv6 address.

Options

- primary*** Clear the static DNS cache entry primary IPv6 address.
- secondary*** Clear the static DNS cache entry secondary IPv6 address.

Example

```
no address ipv6 primary
no address ipv6 secondary
```

Syntax

```
address ipv6 { primary <IPV6_HOST> | secondary <IPV6_HOST> }
```

Mode

DNS Proxy Static DNS Cache

Description

Set the static DNS cache entry IPv6 address.

Options

- primary** Primary address.
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*
- secondary** Secondary address.
- <IPV6_HOST>** IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*

Example

```
address ipv6 primary 2016::2016
address ipv6 secondary 2016::2016
```

Syntax

```
flush cache-entry { ipv4 | ipv6 } { id <DNS_PROXY_DYNAMIC_CACHE_ID> | name <DNS_PROXY_CACHE_NAME> }
```

Mode

DNS proxy

Description

Flush the dynamic DNS cache entry.

Options

- ipv4** Flush the specified IPv4 dynamic DNS cache entry.
- ipv6** Flush the specified IPv6 dynamic DNS cache entry.
- id** Specified dynamic DNS cache entry by id.
- <DNS_PROXY_DYNAMIC_CACHE_ID>** Dynamic DNS cache domain name.
Example: *sonicwall.com*
- name** Specified dynamic DNS cache entry by id.
- <DNS_PROXY_CACHE_NAME>** DNS proxy cache domain name.
Example: *sonicwall.com*

Example

```
flush cache-entry ipv4 sonicwall.com
flush cache-entry ipv6 ipv6.google.com
```

Syntax

```
flush cache-entries { ipv4 | ipv6 }
```

Mode

DNS proxy

Description

Flush all the dynamic DNS cache entries.

Options

ipv4 Flush all the IPv4 dynamic DNS cache entries.

ipv6 Flush all the IPv6 dynamic DNS cache entries.

Example

```
flush cache-entries ipv4
flush cache-entries ipv6
```

Syntax

```
vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress
interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> }
```

Mode

Config

Description

Add/edit VLAN translation and enter its configuration mode.

Options

ingress	VLAN translation ingress.
interface	Ingress interface.
<VLAN_TRANSLATION_INGRESS_IFACE_NAME>	Ingress interface name. Example: <i>X0</i>
vlan	Ingress VLAN tag.
<VLAN_TRANSLATION_INGRESS_VLAN_ID>	Interface VLAN id. Example: <i>23</i>
egress	VLAN translation egress.
interface	Egress interface.
<VLAN_TRANSLATION_EGRESS_IFACE_NAME>	Egress interface name. Example: <i>X0</i>
vlan	Egress VLAN tag.
<VLAN_TRANSLATION_EGRESS_VLAN_ID>	Interface VLAN id. Example: <i>23</i>

Example

```
vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
```

Syntax

```
no vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress
interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> }
```

Mode

Config

Description

Delete one VLAN translation.

Options

ingress	VLAN translation ingress.
interface	Ingress interface.
<VLAN_TRANSLATION_INGRESS_IFACE_NAME>	Ingress interface name. Example: <i>X0</i>
vlan	Ingress VLAN tag.
<VLAN_TRANSLATION_INGRESS_VLAN_ID>	Interface VLAN id. Example: <i>23</i>
egress	VLAN translation egress.
interface	Egress interface.

<VLAN_TRANSLATION_EGRESS_IFACE_NAME>	Egress interface name. Example: <i>X0</i>
vlan	Egress VLAN tag.
<VLAN_TRANSLATION_EGRESS_VLAN_ID>	Interface VLAN id. Example: <i>23</i>

Example

```
no vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
```

Syntax

```
no vlan-translations
```

Mode

Config

Description

Delete all VLAN translations.

Example

```
no vlan-translations
```

Syntax

```
ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME>
```

Mode

VLAN Translation

Description

Set VLAN translation ingress interface.

Options

<VLAN_TRANSLATION_INGRESS_IFACE_NAME>	Ingress interface name. Example: <i>X0</i>

Example

```
ingress interface X1
```

Syntax

```
ingress vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID>
```

Mode

VLAN Translation

Description

Set VLAN translation ingres VLAN id.

Options

<VLAN_TRANSLATION_INGRESS_VLAN_ID>	Interface VLAN id. Example: <i>23</i>

Example

```
ingress vlan 111
```

Syntax

```
egress interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME>
```

Mode

VLAN Translation

Description

Set VLAN translation egress interface.

Options

<VLAN_TRANSLATION_EGRESS_IFACE_NAME> Egress interface name.
Example: *X0*

Example

```
egress interface X2
```

Syntax

```
egress vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID>
```

Mode

VLAN Translation

Description

Set VLAN translation egress VLAN id.

Options

<VLAN_TRANSLATION_EGRESS_VLAN_ID> Interface VLAN id.
Example: *23*

Example

```
egress vlan 222
```

Syntax

```
reverse
```

Mode

VLAN Translation

Description

Enable reverse translation.

Example

```
reverse
```

Syntax

```
no reverse
```

Mode

VLAN Translation

Description

Disable reverse translation.

Example

no reverse

Syntax

dns-security

Mode

Config

Description

Configure and enter DNS security mode.

Example

dns-security

Syntax

dns-sinkhole

Mode

DNS Security

Description

Enter DNS Sinkhole mode.

Example

dns-sinkhole

Syntax

enable

Mode

DNS Sinkhole

Description

Enable DNS Sinkhole.

Example

enable

Syntax

no enable

Mode

DNS Sinkhole

Description

Disable DNS Sinkhole.

Example

no enable

Syntax

```
action-type { dropping-with-dns-reply-of-forged-ip <IPV4_HOST> <IPV6_HOST> | dropping-with-logs | dropping-with-negative-dns-reply-to-source }
```

Mode

DNS Sinkhole

Description

Set action type.

Options

<i>dropping-with-dns-reply-of-forged-ip</i> <i><IPV4_HOST></i>	Dropping, with DNS reply of Forged IP IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i><IPV6_HOST></i>	IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>dropping-with-logs</i>	Dropping, with Logs
<i>dropping-with-negative-dns-reply-to-source</i>	Dropping, with negative DNS reply to Source

Example

```
action-type dropping-with-logs
action-type dropping-with-negative-dns-reply-to-source
action-type dropping-with-dns-reply-of-forged-ip 127.0.0.1 ::1
```

Syntax

```
no custom-malicious-entries
```

Mode

DNS Sinkhole

Description

Delete all the custom malicious entries.

Example

```
no custom-malicious-entries
```

Syntax

```
no custom-malicious-entry <DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME>
```

Mode

DNS Sinkhole

Description

Delete the specified custom malicious entry.

Options

<i><DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME></i>	Custom malicious domain name. Example: <i>sonicwall.com</i>

Example

```
no custom-malicious-entry sonicwall.com
```

Syntax

custom-malicious-entry <DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME>

Mode

DNS Sinkhole

Description

Add custom malicious entry.

Options

<DNS_SINKHOLE_CUSTOM_MALI_DOMAIN_NAME> Custom malicious domain name.
Example: *sonicwall.com*

Example

custom-malicious-entry sonicwall.com

Syntax

no white-list-entries

Mode

DNS Sinkhole

Description

Delete all the white list entries.

Example

no white-list-entries

Syntax

no white-list-entry <DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME>

Mode

DNS Sinkhole

Description

Delete the specified white list entry.

Options

<DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME> White list domain name.
Example: *baidu.com*

Example

no white-list-entry sonicwall.com

Syntax

white-list-entry <DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME>

Mode

DNS Sinkhole

Description

Add white list entry.

Options

<DNS_SINKHOLE_WHITE_LIST_DOMAIN_NAME> White list domain name.
Example: *baidu.com*

Example

```
white-list-entry sonicwall.com
```

Syntax

```
dns-tunnel
```

Mode

DNS Security

Description

Enter DNS Tunnel mode.

Example

```
dns-tunnel
```

Syntax

```
enable
```

Mode

DNS Tunnel

Description

Enable DNS Tunnel detection.

Example

```
enable
```

Syntax

```
no enable
```

Mode

DNS Tunnel

Description

Disable DNS Tunnel detection.

Example

```
no enable
```

Syntax

```
block-all
```

Mode

DNS Tunnel

Description

Block DNS traffic for all the detected clients.

Example

```
block-all
```

Syntax

```
no block-all
```

Mode

DNS Tunnel

Description

Disable the operation of block DNS traffic.

Example

```
no block-all
```

Syntax

```
no white-list-entries
```

Mode

DNS Tunnel

Description

Delete all the white list entries.

Example

```
no white-list-entries
```

Syntax

```
no white-list-entry <IPV4_HOST>
```

Mode

DNS Tunnel

Description

Delete the specified white list entry.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
no white-list-entry 10.10.10.1
```

Syntax

```
white-list-entry <IPV4_HOST>
```

Mode

DNS Tunnel

Description

Add white list entry.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
white-list-entry 10.10.10.1
```

Syntax

```
block <IPV4_HOST>
```

Mode

DNS Tunnel

Description

Block DNS traffic for detected client per demand.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
block ip 10.10.10.1
```

Syntax

```
no block <IPV4_HOST>
```

Mode

DNS Tunnel

Description

Disable the operation of block DNS traffic for detected client per demand.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
block ip 10.10.10.1
```

Syntax

```
portshield-groups
```

Mode

Config

Description

Configure and enter PortShield Groups mode.

Example

```
portshield-groups
```

Syntax

```
no external-switch <UINT32>
```

Mode

PortShield Groups

Description

Delete specified portshield group external switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
no external-switch 1
```

Syntax

```
no external-switches
```

Mode

PortShield Groups

Description

Delete all portshield group external switches.

Example

```
no external-switches
```

Syntax

```
external-switch <UINT32>
```

Mode

PortShield Groups

Description

Add/edit a external switch and enter its configuration mode.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
external-switch 1
```

Syntax

id <UINT32>

Mode

External Switch

Description

Index of the Extended Switch Instance.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

id 1

Syntax

switch-model { n1108p-on | n1108t-on | n1124p-on | n1124t-on | n1148p-on | n1148t-on | n1524 | n1524p | n1548 | n1548p | n2024 | n2024p | n2048 | n2048p | n2128px-on | n3024 | n3024f | n3024p | n3048 | n3048p | n3132px-on | x1008 | x1008p | x1018 | x1018p | x1026 | x1026p | x1052 | x1052p | x4012 }

Mode

External Switch

Description

Select Model of the Switch configured in the Extended Switch Instance.

Options

n1108p-on Model N1108P-ON.

n1108t-on Model N1108T-ON.

n1124p-on Model N1124P-ON.

n1124t-on Model N1124T-ON.

n1148p-on Model N1148P-ON.

n1148t-on Model N1148T-ON.

n1524 Model N1524.

n1524p Model N1524P.

n1548 Model N1548.

n1548p Model N1548P.

n2024 Model N2024.

n2024p Model N2024P.

n2048 Model N2048.

n2048p Model N2048P.

n2128px-on Model N2128PX-ON.

n3024 Model N3024.

n3024f Model N3024F.

<i>n3024p</i>	Model N3024P.
<i>n3048</i>	Model N3048.
<i>n3048p</i>	Model N3048P.
<i>n3132px-on</i>	Model N3132PX-ON.
<i>x1008</i>	Model X1008.
<i>x1008p</i>	Model X1008P.
<i>x1018</i>	Model X1018.
<i>x1018p</i>	Model X1018P.
<i>x1026</i>	Model X1026.
<i>x1026p</i>	Model X1026P.
<i>x1052</i>	Model X1052.
<i>x1052p</i>	Model X1052P.
<i>x4012</i>	Model X4012.

Example

```
switch-model x1008
```

Syntax

```
ip <IPV4_HOST>
```

Mode

External Switch

Description

Set IPv4 Address of the Switch configured in the Extended Switch Instance.

Options

```
<IPV4_HOST>  IPV4 Address in the form: a.b.c.d.  
Example: 192.168.168.168
```

Example

```
ip 10.10.10.200
```

Syntax

```
user-name <WORD>
```

Mode

External Switch

Description

Set Extended Switch Username.

Options

```
<WORD>  Word in the form: WORD or \"QUOTED STRING\".  
Example: abc
```

Example

```
user-name admin
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

External Switch

Description

Set Extended Switch Password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password pwd1234
```

Syntax

```
switch-mode { daisy-chain | standalone }
```

Mode

External Switch

Description

Select Extended Switch Mode - Standalone or DaisyChain.

Options

daisy-chain Daisy chain mode.

standalone Standalone mode.

Example

```
switch-mode standalone
```

Syntax

```
parent-switch-id <UINT32>
```

Mode

External Switch

Description

Index of the Extended Switch Instance.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
parent-switch-id 1
```

Syntax

parent-switch-uplink <UINT32>

Mode

External Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

parent-switch-uplink 1

Syntax

no parent-switch-uplink

Mode

External Switch

Description

Clear Extended Switch Interface connected to the Standalone/Primary Firewall.

Example

no parent-switch-uplink

Syntax

switch-management <UINT32>

Mode

External Switch

Description

Set Interface of the Firewall via which the Extended Switch is managed.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

switch-management 1

Syntax

secondary-switch-management <UINT32>

Mode

External Switch

Description

Set Management Interface of the Extended Switch connected to the Secondary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
secondary-switch-management 1
```

Syntax

```
firewall-uplink <CONFIGURABLE_INTERFACE>
```

Mode

External Switch

Description

Set Firewall Interface connected to the Extended Switch.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
firewall-uplink X0
```

Syntax

```
no firewall-uplink
```

Mode

External Switch

Description

Clear Firewall Interface connected to the Extended Switch.

Example

```
no firewall-uplink
```

Syntax

```
switch-uplink <UINT32>
```

Mode

External Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

switch-uplink 1

Syntax

no switch-uplink

Mode

External Switch

Description

Clear Extended Switch Interface connected to the Standalone/Primary Firewall.

Example

no switch-uplink

Syntax

secondary-switch-uplink <UINT32>

Mode

External Switch

Description

Set Uplink Interface of the Extended Switch connected to the Secondary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

secondary-switch-uplink 1

Syntax

no secondary-switch-uplink

Mode

External Switch

Description

Clear Uplink Interface of the Extended Switch connected to the Secondary Firewall.

Example

no secondary-switch-uplink

Syntax

stp-mode { classic | multiple | pvst | rapid | rapid-pvst }

Mode

External Switch

Description

Select STP Operation Mode configured on the Extended Switch.

Options

<i>classic</i>	Classic mode.
<i>multiple</i>	Multiple mode.
<i>pvst</i>	pvst mode.
<i>rapid</i>	Rapid mode.
<i>rapid-pvst</i>	rapid-pvst mode.

Example

```
stp-mode classic
```

Syntax

```
stp-state
```

Mode

External Switch

Description

Enable Global STP State configured on the Extended Switch.

Example

```
stp-state
```

Syntax

```
no stp-state
```

Mode

External Switch

Description

Disable Global STP State configured on the Extended Switch.

Example

```
no stp-state
```

Syntax

```
poe-alert-usage-threshold <UINT32>
```

Mode

External Switch

Description

Set PoE Alert Usage Threshold configured on the Extended Switch.

Options

<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

poe-alert-usage-threshold 1

Syntax

poe-traps

Mode

External Switch

Description

Enable PoE Traps configured on the Extended Switch.

Example

poe-traps

Syntax

no poe-traps

Mode

External Switch

Description

Disable PoE Traps configured on the Extended Switch.

Example

no poe-traps

Syntax

poe-power-limit-mode { class-limit | port-limit }

Mode

External Switch

Description

Select PoE Power Limit Mode configured on the Extended Switch.

Options

class-limit Class limit mode.

port-limit Port limit mode.

Example

poe-power-limit-mode port-limit

Syntax

poe-management-mode { class | dynamic | static }

Mode

External Switch

Description

Select PoE Management Mode configured on N series Switch.

Options

- class** Class mode.
- dynamic** Dynamic mode.
- static** Static mode.

Example

```
poe-management-mode dynamic
```

Syntax

```
poe-detection-type { dot3at+legacy | legacy }
```

Mode

External Switch

Description

Select PoE Detection Type configured on N series Switch.

Options

- dot3at+legacy** Dot3at+Legacy mode.
- legacy** Legacy mode.

Example

```
poe-detection-type legacy
```

Syntax

```
show tunnel-interface 4to6 <TUNNEL6_TUNNEL_INTERFACE> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show 4to6 tunnel interface configuration.

Options

- <TUNNEL6_TUNNEL_INTERFACE>** Tunnel6 tunnel interface name.
Example: *tunnel6TunnelInterface*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.
- status** MTU status for tunnel interface.

Example

```
show tunnel-interface tunnel CorpVPNTunnel
```

Syntax

```
show tunnel-interfaces 4to6 [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all 4to6 tunnel interfaces configuration.

Options

pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	MTU status for tunnel interface.

Example

```
show tunnel-interfaces 4to6
```

Syntax

```
show interfaces [ [ ipv4 | ipv6 ] [ { { { base | extra-ip | physical | prefixes | vlan [ parent <CONFIGURABLE_INTERFACE> ] } } [ pending-config ] } | ips | statistics | status } ] | display-all-traffic | mac ]
```

Mode

All Modes

Description

Show all interfaces.

Options

ipv4	Show all IPv4 interfaces.
ipv6	Show all IPv6 interfaces.
base	Show interface base configuration.
extra-ip	Show IPv6 interface extra IP addresses.
physical	Show physical interfaces.
prefixes	Show IPv6 interface prefixes.
vlan	Show VLAN interfaces.
parent	Show VLAN interfaces under specified parent interface.
<CONFIGURABLE_INTERFACE>	Interface name. Example: <i>X0</i>
pending-config	Show pending configuration changes.
ips	Show interfaces IP.
statistics	Show interfaces statistics.
status	Show interfaces status.
display-all-traffic	Show interface statistics option.

mac Show interfaces MAC.

Example

```
show interfaces
```

Syntax

```
show interface [ ipv4 | ipv6 ] <CONFIGURABLE_INTERFACE> [ vlan <VLAN_TAG> ] [ tunnel <WLAN_TUNNEL_ID> ] [ { base | extra-ip |  
ips | mac | pending-config | prefixes | statistics | status } ]
```

Mode

All Modes

Description

Show interface configuration.

Options

ipv4	Show IPv4 interface configuration.
ipv6	Show IPv6 interface configuration.
<CONFIGURABLE_INTERFACE>	Interface name. Example: <i>X0</i>
vlan	Sub-interface VLAN.
<VLAN_TAG>	VLAN tag. Example: <i>23</i>
tunnel	Configure WLAN tunnel interface.
<WLAN_TUNNEL_ID>	WLAN tunnel ID. Example: <i>1</i>
base	Show interface base configuration.
extra-ip	Show IPv6 interface extra IP addresses.
ips	Show interface IP.
mac	Show interface MAC.
pending-config	Show pending configuration changes.
prefixes	Show IPv6 interface prefixes.
statistics	Show interface statistics.
status	Show interface status.

Example

```
show interface X1  
show interface X1 vlan 100  
show interface WT0  
show interface X1 tunnel 1  
show interface X1 vlan 100 tunnel 2  
show interface WT1 vlan 200  
show interface ipv6 X1  
show interface ipv6 X1 vlan 100  
show interface ipv6 WT0  
show interface ipv6 X1 tunnel 1  
show interface ipv6 X1 vlan 100 tunnel 2  
show interface ipv6 WT1 vlan 200  
show interface X1 ips  
show interface X1 mac  
show interface X1 statistics  
show interface ipv6 X1 statistics
```

Syntax

show switch-statdump

Mode

All Modes

Description

Show Switch Port Statistic Dump.

Example

show switch-statdump

Syntax

show tunnel-interface vpn <VPN_TUNNEL_INTERFACE> [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show VPN tunnel interface configuration.

Options

<VPN_TUNNEL_INTERFACE> VPN tunnel interface name.
Example: *vpnTunnelInterface*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show VPN tunnel interface status.

Example

show tunnel-interface vpn CorpVPNTunnel
show tunnel-interface vpn CorpVPNTunnel status

Syntax

show tunnel-interfaces vpn [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all VPN tunnel interfaces configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show tunnel-interfaces vpn

Syntax


```
show arp [ base | cache <IPV4_HOST> <INTERFACE_NAME> | caches | entries | entry <ARP_IPV4_HOST> <ARP_MAC> <ARP_INTERFACE> |
statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show ARP status or configuration.

Options

base	Show ARP base configuration.
cache	Show ARP cache.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<INTERFACE_NAME>	Interface name. Example: <i>X0</i>
caches	Show ARP cache.
entries	Show all static ARP entries.
entry	Show a specified static ARP entry.
<ARP_IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<ARP_MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
<ARP_INTERFACE>	Interface name. Example: <i>X0</i>
statistics	Show ARP statistics.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show arp
show arp entries
show arp entry 10.10.10.10 00:01:02:03:04:05 X0
show arp caches
show arp cache 10.10.10.10 X0
show arp statistics
```

Syntax

```
show dns [ [ base | fqdn-binding | fqdn-over-tcp-dns | rebinding | servers [ ipv4 | ipv6 ] | split-entries | split-entry
<DNS_SPLIT_DNS_ENTRY_NAME> | split-servers | wan [ ipv4 | ipv6 ] ] [ { pending-config | with-pending-config } ] | cache [
interface-reverse ] ]
```

Mode

All Modes

Description

Show DNS configuration.

Options

base	Show the global DNS configuration.
fqdn-binding	Show DNS binging for FQDN configuration.
fqdn-over-tcp-dns	Show DNS host name lookup over TCP for FQDN configuration.

rebinding	Show DNS rebinding attack prevention configuration.
servers	Show DNS server configuration.
ipv4	Show IPv4 DNS server configuration.
ipv6	Show IPv6 DNS server configuration.
split-entries	Show all the DNS split DNS entries.
split-entry	Show the specified DNS split DNS entry.
<DNS_SPLIT_DNS_ENTRY_NAME>	Split DNS entry domain name. Example: <i>sonicwall.com</i>
split-servers	Show split DNS server configuration.
wan	Show WAN DNS detail.
ipv4	Show IPv4 WAN DNS server detail.
ipv6	Show IPv6 WAN DNS server detail.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
cache	Show DNS cache.
interface-reverse	Show interface names reverse DNS cache.

Example

show dns servers

Syntax

show dynamic-dns profiles [ipv4 | ipv6] [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show all dynamic DNS profiles.

Options

ipv4	Show IPv4 dynamic DNS profiles.
ipv6	Show IPv6 dynamic DNS profiles.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show all dynamic DNS profiles status.

Example

show dynamic-dns profiles

Syntax

show dynamic-dns profile [ipv4 | ipv6] <DDNS_PROFILE_NAME> [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show dynamic DNS profile.

Options

ipv4	Show IPv4 dynamic DNS profile.
ipv6	Show IPv6 dynamic DNS profile.
<DDNS_PROFILE_NAME>	Dynamic DNS profile name. Example: <i>mydns</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show a dynamic DNS profile status.

Example

show dynamic-dns profile DynDNS.org

Syntax

```
show dhcp-server [ [ ipv6 [ [ base | leases [ statistic ] | option { { group <DHCP_OPTION_GROUP> | groups | object
<DHCP_OPTION_OBJECT> | objects } } | scope { { dynamic <DHCP_IPV6_DYNAMIC_SCOPE_NAME> | static <DHCP_IPV6_STATIC_SCOPE_NAME> }
} | scopes { { dynamic | static } } ] ] ] | [ ipv4 ] [ [ base | leases [ statistic ] | option { { group <DHCP_OPTION_GROUP> |
groups | object <DHCP_OPTION_OBJECT> | objects } } | scope { { dynamic <SCOPE_START_IPV4_HOST> <SCOPE_END_IPV4_HOST> | static
<STATIC_SCOPE_IPV4_HOST> <STATIC_SCOPE_MAC> } } | scopes { { dynamic | static } } ] ] ] [ { pending-config | with-pending-
config } ] ]
```

Mode

All Modes

Description

Show DHCP server configuration.

Options

ipv6	Show IPv6 DHCP server configuration.
base	Show IPv6 DHCP server base configuration.
leases	Show IPv6 DHCP server leases.
statistic	Show IPv6 DHCP server leases status.
option	IPv6 DHCP server option configuration.
group	Specify option group.
<DHCP_OPTION_GROUP>	DHCP server option group name. Example: <i>Corp Network DHCP Group</i>
groups	IPv6 DHCP server all option groups.
object	Specify option object.
<DHCP_OPTION_OBJECT>	DHCP server option object name. Example: <i>Corp Network DHCP Options</i>
objects	IPv6 DHCP server all option objects.
scope	IPv6 DHCP server static or dynamic scope.

dynamic	IPv6 DHCP server dynamic configuration.
<DHCP_IPV6_DYNAMIC_SCOPE_NAME>	IPv6 DHCP server dynamic scope name. Example: <i>abc</i>
static	IPv6 DHCP server static configuration.
<DHCP_IPV6_STATIC_SCOPE_NAME>	IPv6 DHCP server static scope name. Example: <i>abc</i>
scopes	IPv6 DHCP server all static or dynamic scopes.
dynamic	IPv6 DHCP server dynamic configuration.
static	IPv6 DHCP server static configuration.
ipv4	Show IPv4 DHCP server configuration.
base	Show IPv4 DHCP server base configuration.
leases	Show DHCP server leases.
statistic	Show DHCP server leases status.
option	DHCP server option configuration.
group	Specify option group.
<DHCP_OPTION_GROUP>	DHCP server option group name. Example: <i>Corp Network DHCP Group</i>
groups	All option groups.
object	Specify option object.
<DHCP_OPTION_OBJECT>	DHCP server option object name. Example: <i>Corp Network DHCP Options</i>
objects	All option objects.
scope	DHCP server static or dynamic scope.
dynamic	DHCP server dynamic configuration.
<SCOPE_START_IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<SCOPE_END_IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
static	DHCP server static configuration.
<STATIC_SCOPE_IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<STATIC_SCOPE_MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
scopes	DHCP server all static or dynamic scopes.
dynamic	DHCP server dynamic configuration.
static	DHCP server static configuration.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show dhcp-server
```

Syntax

```
show failover-lb [ base | group <FLB_GROUP_NAME> | groups | responder | statistics [ group <FLB_GROUP_NAME> ] | status [ group <FLB_GROUP_NAME> | groups | member <FLB_GROUP_NAME> | members ] ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show failover and load balancing status or configuration.

Options

base	Show failover and load balancing base configuration.
group <FLB_GROUP_NAME>	Show failover and load balancing group configuration. Failover & LB group name. Example: <i>myFLBGroup</i>
groups	Show failover and load balancing groups configuration.
responder	Show status for respond to probes.
statistics group <FLB_GROUP_NAME>	Show failover and load balancing statistics. Show statistics of a specified failover and load balancing group. Failover & LB group name. Example: <i>myFLBGroup</i>
status	Show status of failover and load balancing.
group <FLB_GROUP_NAME>	Show status of a specified failover and load balancing group. Failover & LB group name. Example: <i>myFLBGroup</i>
groups	Show status of all failover and load balancing groups.
member <FLB_GROUP_NAME>	Show status of a specified failover and load balancing group member. Failover & LB group name. Example: <i>myFLBGroup</i>
members	Show status of all failover and load balancing group members.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show failover-lb
show failover-lb status
show failover-lb statistics
```

Syntax

```
show ip-helper [ { policies | policy protocol <IPH_PROTOCOL> source { group <ADDR_GROUP_NAME> | interface <IPH_INTERFACE> |
name <ADDR_NETWORK_NAME> | zone <ZONE_NO_MULTICAST_NAME> } | protocol <IPH_PROTOCOL> | protocols } [ statistics ] | base |
dhcp-relay-leases | dhcpv6-relay-leases } [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IP helper status or configuration.

Options

policies	Show all IP helper policies.
policy	Show IP helper policy.

protocol	Specify the IP helper relay protocol.
<IPH_PROTOCOL>	IP Helper relay protocol name. Example: <i>mydns</i>
source	Specify source.
group	IP helper policy source address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
interface	IP helper policy source interface.
<IPH_INTERFACE>	IP helper interface name. Example: <i>X1</i>
name	IP helper policy source address object name.
<ADDR_NETWORK_NAME>	Network address object name. Example: <i>Sales Network</i>
zone	IP helper policy source zone.
<ZONE_NO_MULTICAST_NAME>	Zone object name. Example: <i>DMZ</i>
protocol	Show an IP helper relay protocol.
<IPH_PROTOCOL>	IP Helper relay protocol name. Example: <i>mydns</i>
protocols	Show all IP helper relay protocols.
statistics	Show statistics for policies or specified protocol.
base	Show IP helper base configuration.
dhcp-relay-leases	Show all IP helper DHCP relay leases.
dhcpv6-relay-leases	Show all IP helper DHCPv6 relay leases.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show ip-helper
```

Syntax

```
show mac-ip-anti-spoof [ ipv4 | ipv6 ] [ cache { { entries [ status ] | entry <MAC_IP_ANTI_SPOOF_STATIC_IP>
<MAC_IP_ANTI_SPOOF_STATIC_MAC> <MAC_IP_ANTI_SPOOF_STATIC_INTERFACE> } } | detected-list | interface
<MAC_IP_ANTI_SPOOF_INTERFACE> | interfaces | lookup-statistics } [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show MAC-IP anti-spoof configuration and information.

Options

ipv4	Show IPv4 MAC-IP anti-spoof configuration.
ipv6	Show IPv6 MAC-IP anti-spoof configuration.
cache	Show MAC-IP anti-spoof cache.
entries	Show all MAC anti-spoof cache entries.
status	Show all MAC-IP anti-spoof cache entries status.
entry	Show an MAC anti-spoof cache entry.

<MAC_IP_ANTI_SPOOF_STATIC_IP>	MAC-IP anti-spoof static ip. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
<MAC_IP_ANTI_SPOOF_STATIC_MAC>	MAC-IP anti-spoof static mac. Example: <i>00:0C:F1:56:98:AD</i>
<MAC_IP_ANTI_SPOOF_STATIC_INTERFACE>	MAC-IP anti-spoof enabled static interface. Example: <i>X0</i>
detected-list	Show MAC-IP anti-spoof spoof detected list.
interface	Show MAC-IP anti-spoof interface configuration.
<MAC_IP_ANTI_SPOOF_INTERFACE>	MAC-IP anti-spoof interface. Example: <i>X0</i>
interfaces	Show MAC-IP anti-spoof configuration for all interfaces.
lookup-statistics	Show MAC-IP anti-spoof lookup statistics.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show mac-ip-anti-spoof

Syntax

show nat-policies [ipv4 | ipv6 | nat64] [uuid <UUID>] [statistics] [{ custom | default }] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all NAT policies.

Options

ipv4	Show only IPv4 NAT policies.
ipv6	Show only IPv6 NAT policies.
nat64	Show only NAT64 policies.
uuid	Show NAT policy by UUID.
<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
statistics	Show statistics for all nat policies.
custom	Show custom configuration.
default	Show system/factory default configuration.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show nat-policies

Syntax

```
show nat-policy ipv4 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ uuid <UUID> ] [ source { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host
<ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service
{ { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
} ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>
<SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
uuid	Show NAT policy by UUID.
<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
source	Original source ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source ("Original" if not specified).
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Original destination ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
translated-service	Translated service ("Original" if not specified).
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
original	Original service.
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
statistics	Show statistics for specified nat policy.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show nat-policy inbound X3 outbound X4 source any translated-source original destination name "Web Server Public" translated-destination name "Web Server Private" service "My Web Services" translated-service original

Syntax

```
show nat-policy ipv6 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ uuid <UUID> ] [ source { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-destination { { embedded-ipv4-address | group <ADDR_GROUP_NAME> | host
<ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ service
{ { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
} ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN>
<SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IPv6 NAT policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
uuid	Show NAT policy by UUID.
<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
source	Original source ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source ("Original" if not specified).
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Original destination ("Any" if not specified).
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-destination	Translated destination ("Original" if not specified).
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Original service ("Any" if not specified).
any	Any service.
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
icmp-udp-tcp	ICMP UDP TCP service.
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
translated-service	Translated service ("Original" if not specified).
group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
original	Original service.
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
statistics	Show statistics for specified nat policy.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show nat-policy ipv6 inbound X3 outbound X4 source any translated-source original destination name "Web Server Public"
translated-destination name "Web Server Private" service "My Web Services" translated-service original
```

Syntax

```
show nat-policy nat64 inbound <NAT_INTERFACE> outbound <NAT_INTERFACE> [ uuid <UUID> ] [ source { { any | fqdn <ADDR_FQDN> |
group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK>
| range <ADDR_BEGIN> <ADDR_END> } } ] [ translated-source { { group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> |
network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN> <ADDR_END> } } ] [ pref64 { { any | group <ADDR_GROUP_NAME>
| name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> } } ] [ translated-destination { { embedded-ipv4-address | group
<ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | original | range <ADDR_BEGIN>
<ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | icmp-udp-tcp | name <SVC_NAME> | protocol <SVC_PROTOCOL>
<SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ translated-service { { group <SVC_GROUP_NAME> | name <SVC_NAME> | original | protocol
<SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT64 policy.

Options

<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
outbound	Outbound interface.
<NAT_INTERFACE>	Interface name. Example: <i>X0</i>
uuid	Show NAT policy by UUID.
<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
source	Original source.
any	Any host.
fqdn	FQDN.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address object group.
<ADDR_FHNR_GROUP_WITH_MIXED>	FQDN/host/network/range group address object name. Example: <i>Web Server Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
translated-source	Translated source.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original source IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
pref64	Original destination.
any	Any host.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
translated-destination	Translated destination.
embedded-ipv4-address	Embedded ipv4 address.
group	Address object group.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original destination IP.
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

<i>service</i>	Original service.
<i>any</i>	Any service.
<i>group</i> <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>
<i>icmp-udp-tcp</i>	ICMP UDP TCP service.
<i>name</i> <SVC_NAME>	Service object name. Service object name. Example: <i>HTTPS</i>
<i>protocol</i> <SVC_PROTOCOL>	Service object protocol. Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>translated-service</i>	Translated service.
<i>group</i> <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>
<i>name</i> <SVC_NAME>	Service object name. Service object name. Example: <i>HTTPS</i>
<i>original</i>	Original service.
<i>protocol</i> <SVC_PROTOCOL>	Service object protocol. Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>statistics</i>	Show statistics for specified nat policy.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show nat-policy nat64 inbound X3 outbound X4 source any translated-source X1 pref64 name nat64AO translated-destination
embedded-ipv4-address service icmp-udp-tcp translated-service original
```

Syntax

```
show nat-policy ipv4 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

<i><UUID></i>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
<i>pending-config</i>	Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show nat-policy ipv4 uuid 3824336935410777187

Syntax

show nat-policy ipv6 uuid <UUID> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show nat-policy ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

show nat-policy nat64 uuid <UUID> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show NAT policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show nat-policy nat64 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

show network-monitor policies [ipv4 | ipv6] [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show all network monitor policies.

Options

<i>ipv4</i>	Show IPv4 network monitor policies.
<i>ipv6</i>	Show IPv6 network monitor policies.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show all network monitor policies status.

Example

show network-monitor policies

Syntax

show network-monitor policy [ipv4 | ipv6] <NETMON_NAME> [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show network monitor policy.

Options

<i>ipv4</i>	Show IPv4 network monitor policies.
<i>ipv6</i>	Show IPv6 network monitor policy.
<i><NETMON_NAME></i>	Atom Object name. Example: <i>Web Services Monitor</i>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show a specific network monitor policy status.

Example

show network-monitor policy "Remote Servers"

Syntax

show routing mode [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show routing mode.

Options

- pending-config**

Show pending configuration changes.
- with-pending-config**

View current configuration with pending changes included in the output.

Example

show routing mode

Syntax

show route-policies [ipv4 | ipv6] [{ dynamic | system }] [{ custom | default }] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all route policies.

Options

- ipv4**

Show only IPv4 route policies.
- ipv6**

Show only IPv6 route policies.
- dynamic**

Show all dynamic route policies.
- system**

Show all ephemeral system route policies.
- custom**

Show custom configuration.
- default**

Show system/factory default configuration.
- pending-config**

Show pending configuration changes.
- with-pending-config**

View current configuration with pending changes included in the output.

Example

show route-policies

Syntax

show route-policy ipv4 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }] [destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }] [service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }] [gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } }] [tos <ROUTE_HEX_UINT8>] [mask <ROUTE_HEX_UINT8>] [distance { auto | value <UINT8> }] [path-selection-profile <ROUTE_PATH_SELECTION_PROFILE_NAME>] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show a route policy.

Options

- <ROUTING_INTERFACE_NAME>**

Route interface name.
Example: *X0*
- metric**

Route policy metric.
- <UINT8>**

Integer in the form: D OR 0xHH.
Example: *123*
- source**

Route policy source.

any	Any host.
group <ADDR_GROUP_NAME>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_HOST_NETWORK_RANGE_NAME>	Address object name. Host/network/range address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN> <ADDR_END>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Route policy destination.
any	Any host.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_WITH_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_FHNR_NAME_WITH_MIXED>	Address object name. FQDN/host/network/range address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN> <ADDR_END>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Route policy service.
any	Any service.
group <SVC_GROUP_NAME>	Service group. Service object group name. Example: <i>VOIP</i>

name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
path-selection-profile	Route policy SD-WAN path selection profile.
<ROUTE_PATH_SELECTION_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show route-policy interface X4 metric 255 service name "FTP"
```

Syntax

```
show route-policy ipv6 interface <ROUTING_INTERFACE_NAME> metric <UINT8> [ source { { any | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_HOST_NETWORK_RANGE_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ destination { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | name <ADDR_FHNR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ gateway { { default | host <ADDR_HOST> | name <ADDR_HOST_NAME> } } ] [ tos <ROUTE_HEX_UINT8> ] [ mask <ROUTE_HEX_UINT8> ] [ distance { auto | value <UINT8> } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv6 route policy.

Options

<ROUTING_INTERFACE_NAME>	Route interface name. Example: <i>X0</i>
metric	Route policy metric.

<UINT8>	Integer in the form: D OR 0xHH. Example: 123
source	Route policy source.
any	Any host.
group	Address group name.
<ADDR_GROUP_NAME>	Group address object name. Example: Sales Group
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NETWORK_RANGE_NAME>	Host/network/range address object name. Example: Web Server
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
destination	Route policy destination.
any	Any host.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: example.com
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: Sales Group
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_FHNR_NAME_WITH_MIXED>	FQDN/host/network/range address object name. Example: Web Server
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
service	Route policy service.
any	Any service.

group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
gateway	Route policy gateway.
default	Default gateway 0.0.0.0/::
host	Gateway IP.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_HOST_NAME>	Host address object name. Example: <i>Web Server</i>
tos	Route policy TOS.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
mask	Route policy TOS mask.
<ROUTE_HEX_UINT8>	Hexadecimal integer in the form: 0xHH. Example: <i>0xaa</i>
distance	Route policy admin distance.
auto	Route policy auto admin distance.
value	Route policy custom admin distance.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show route-policy ipv6 interface X4 metric 255 service name "FTP"
```

Syntax

```
show route-policy ipv4 uuid <UUID>
```

Mode

All Modes

Description

Show an IPv4 route policy by associated ID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
show route-policy ipv4 id 3
```

Syntax

```
show route-policy ipv6 uuid <UUID>
```

Mode

All Modes

Description

Show an IPv6 route policy by associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
show route-policy ipv6 id 3
```

Syntax

```
show routing nsm [ database | interface ]
```

Mode

All Modes

Description

Show routing NSM status or configuration.

Options

database Database summary.

interface Interface status and configuration.

Example

```
show routing nsm
```

Syntax

```
show routing rip [ database ]
```

Mode

All Modes

Description

Show routing RIP status or configuration.

Options

database Database summary.

Example

```
show routing rip
```

Syntax

```
show routing ospf [ database | neighbor | routes ]
```

Mode

All Modes

Description

Show routing OSPF status or configuration.

Options

database Database summary.

neighbor Neighbor list.

routes OSPF routing table.

Example

```
show routing ospf
```

Syntax

```
show routing bgp [ neighbor | summary | unicast ]
```

Mode

All Modes

Description

Show routing BGP status or configuration.

Options

neighbor Neighbor list.

summary Summary of BGP neighbor status.

unicast

Example

```
show routing bgp
```

Syntax

```
show routing ripng [ database ]
```

Mode

All Modes

Description

Show routing RIPNG status or configuration.

Options

database Database summary.

Example

```
show routing ripng
```

Syntax

```
show routing ospfv3 [ database | neighbor | routes ]
```

Mode

All Modes

Description

Show routing OSPFv3 status or configuration.

Options

database Database summary.

neighbor Neighbor list.

routes OSPF routing table.

Example

```
show routing ospfv3
```

Syntax

```
show web-proxy [ base | proxy-server <USER_NETPROXY_SERVER> | proxy-servers ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show web proxy configuration.

Options

base Show web proxy base settings.

proxy-server Show an specific proxy server.
<USER_NETPROXY_SERVER> User net proxy server.
Example: *abc*

proxy-servers Show web user proxy servers settings.

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show web-proxy
```

Syntax

```
show amazon-web-services connection [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Amazon Web Services configuration.

Options

- pending-config***

Show pending configuration changes.
- with-pending-config***

View current configuration with pending changes included in the output.

Example

show amazon-web-services

Syntax

show amazon-web-services objects [base | group-mapping <AWS_GROUP_MAPPING_INDEX> | group-mappings]

Mode

All Modes

Description

Show Amazon Web Services status.

Options

- base***

Show Amazon Web Services objects configuration.
- group-mapping***
<AWS_GROUP_MAPPING_INDEX>

Show Amazon Web Services objects address group mapping configuration.
Integer in the form: D OR 0xHHHHHHHHH.
Example: *1*
- group-mappings***

Show Amazon Web Services objects address group mapping configuration.

Example

show amazon-web-services objects

Syntax

show ndp [base | cache | entries | entry <NDP_IPV6_HOST> <NDP_MAC> <NDP_INTERFACE>] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show NDP status or configuration.

Options

- base***

Show NDP base configuration.
- cache***

Show NDP caches.
- entries***

Show all static NDP entries.
- entry***
<NDP_IPV6_HOST>
<NDP_MAC>
<NDP_INTERFACE>

Show a static NDP entry.
IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*
MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*
Interface name.
Example: *X0*
- pending-config***

Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ndp entries
show ndp
show ndp entry 2001:10:10:10:2D0:02BB:03CC:04DD 02:BB:03:CC:04:DD X0
show ndp cache
```

Syntax

```
show tunnel-interface ipv6 <IPV6_TUNNEL_INTERFACE> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show IPv6 tunnel interface configuration.

Options

- <IPV6_TUNNEL_INTERFACE>** IPv6 Interface name.
Example: *myTunnelInterface*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show tunnel-interface ipv6 CorpIPv6Tunnel
```

Syntax

```
show tunnel-interfaces ipv6 [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all IPv6 tunnel interfaces configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show tunnel-interfaces ipv6
```

Syntax

```
show dns-proxy [ [ base | cache-entries | cache-entry <DNS_PROXY_STATIC_DNS_CACHE_NAME> ] [ { pending-config | with-pending-config } ] | status { cache { ipv4 | ipv6 } <DNS_PROXY_CACHE_NAME> | caches { { ipv4 | ipv6 } } | server | split-entries | split-entry <DNS_SPLIT_DNS_ENTRY_NAME> } ]
```

Mode

All Modes

Description

Show DNS proxy configuration and status.

Options

<i>base</i>	Show DNS proxy basic configuration.
<i>cache-entries</i>	Show all the staic DNS cache entries.
<i>cache-entry</i> <DNS_PROXY_STATIC_DNS_CACHE_NAME>	Show the specified static DNS cache entry. Static DNS cache domain name. Example: <i>sonicwall.com</i>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show the DNS proxy status.
<i>cache</i>	Show the specified DNS cache status.
<i>ipv4</i>	Show the specified IPv4 DNS cache status.
<i>ipv6</i> <DNS_PROXY_CACHE_NAME>	Show the specified IPv6 DNS cache status. DNS proxy cache domain name. Example: <i>sonicwall.com</i>
<i>caches</i>	Show all the DNS caches status
<i>ipv4</i>	Show all the IPv4 DNS caches status.
<i>ipv6</i>	Show all the IPv6 DNS caches status.
<i>server</i>	Show the DNS proxy DNS server status.
<i>split-entries</i>	Show all the DNS proxy split DNS entries status.
<i>split-entry</i> <DNS_SPLIT_DNS_ENTRY_NAME>	Show the specified DNS proxy split DNS entry status. Split DNS entry domain name. Example: <i>sonicwall.com</i>

Example

```
show dns-proxy
show dns-proxy cache-entry sonicwall.com
show dns-proxy cache-entries
show dns-proxy status server
show dns-proxy status split-entry sonicwall.com
show dns-proxy status split-entries
show dns-proxy status cache ipv4 sonicwall.com
show dns-proxy status cache ipv6 ipv6.google.com
show dns-proxy status caches ipv4
```

Syntax

```
show vlan-translation { ingress interface <VLAN_TRANSLATION_INGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_INGRESS_VLAN_ID> egress
interface <VLAN_TRANSLATION_EGRESS_IFACE_NAME> vlan <VLAN_TRANSLATION_EGRESS_VLAN_ID> } [ { pending-config | with-pending-
config } | status ]
```

Mode

All Modes

Description

Show VLAN translation configuration or status.

Options

<i>ingress</i>	VLAN translation ingress.
<i>interface</i>	Ingress interface.
<i><VLAN_TRANSLATION_INGRESS_IFACE_NAME></i>	Ingress interface name. Example: <i>X0</i>
<i>vlan</i>	Ingress VLAN tag.
<i><VLAN_TRANSLATION_INGRESS_VLAN_ID></i>	Interface VLAN id. Example: <i>23</i>
<i>egress</i>	VLAN translation egress.
<i>interface</i>	Egress interface.
<i><VLAN_TRANSLATION_EGRESS_IFACE_NAME></i>	Egress interface name. Example: <i>X0</i>
<i>vlan</i>	Egress VLAN tag.
<i><VLAN_TRANSLATION_EGRESS_VLAN_ID></i>	Interface VLAN id. Example: <i>23</i>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show VLAN translation configuration status.

Example

```
show vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222
show vlan-translation ingress interface X1 vlan 111 egress interface X2 vlan 222 status
```

Syntax

```
show vlan-translations [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show all VLAN translations configuration or status.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show all VLAN translations status.

Example

```
show vlan-translations
show vlan-translations status
```

Syntax

```
show dns-security [ [ dns-sinkhole [ { base | custom-malicious-entries | white-list-entries } ] | dns-tunnel [ { base | white-list-entries } ] ] [ { pending-config | with-pending-config } ] | status { sinkhole-statistical | tunnel-clients } ]
```

Mode

All Modes

Description

Show DNS Security configuration.

Options

<i>dns-sinkhole</i>	Show DNS Sinkhole configuration.
<i>base</i>	Show DNS Sinkhole base settings.
<i>custom-malicious-entries</i>	Show DNS Sinkhole custom malicious entries configuration.
<i>white-list-entries</i>	Show DNS Sinkhole white list entries configuration.
<i>dns-tunnel</i>	Show DNS Tunnel detection configuration.
<i>base</i>	Show DNS Tunnel base settings.
<i>white-list-entries</i>	Show DNS Tunnel white list entries configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show the DNS Security status.
<i>sinkhole-statistical</i>	Show the DNS Security DNS Sinkhole statistical status.
<i>tunnel-clients</i>	Show the DNS Security DNS tunnel detected clients status.

Example

```
show dns-security
show dns-security dns-sinkhole
show dns-security dns-tunnel
show dns-security status sinkhole-statistical
show dns-security status tunnel-clients
```

Syntax

```
show portshield-groups [ external-switch <UINT32> | external-switch-diagnostics { { firmware-management | statistics } } |
external-switches ]
```

Mode

All Modes

Description

Show portshield groups configuration.

Options

<i>external-switch</i> <i><UINT32></i>	Show a portshield group external switch object configuration. Integer in the form: D OR 0xHHHHHHHH. Example: 123
<i>external-switch-diagnostics</i>	Show portshield group external switch diagnostics.
<i>firmware-management</i>	Show portshield group external switch diagnostics firmware management.
<i>statistics</i>	Show portshield group external switch diagnostics statistics.
<i>external-switches</i>	Show portshield group external switches configuration.

Example

```
show portshield-groups
```

Syntax

```
show portshield port-configuration
```

Mode

All Modes

Description

Show portshield port configuration.

Options

port-configuration Show portshield port configuration.

Example

```
show portshield port configuration
```

Syntax

```
firewall
```

Mode

Config

Description

Configure firewall settings.

Example

```
firewall
```

Syntax

```
security-services-enforcement global
```

Mode

All Modes

Description

Set security services enforcement as global mode.

Example

```
security-services-enforcement global
```

Syntax

```
security-services-enforcement policy
```

Mode

All Modes

Description

Set security services enforcement as policy mode.

Example

```
security-services-enforcement policy
```

Syntax

stealth-mode

Mode

All Modes

Description

Enable stealth mode.

Example

stealth-mode

Syntax

no stealth-mode

Mode

All Modes

Description

Disable stealth mode.

Example

no stealth-mode

Syntax

randomize-id

Mode

All Modes

Description

Enable randomize IP ID.

Example

randomize-id

Syntax

no randomize-id

Mode

All Modes

Description

Disable randomize IP ID.

Example

no randomize-id

Syntax

decrement ttl

Mode

All Modes

Description

Enable decrement IP TTL for forwarded traffic.

Example

```
decrement ttl
```

Syntax

```
no decrement ttl
```

Mode

All Modes

Description

Disable decrement IP TTL for forwarded traffic.

Example

```
no decrement ttl
```

Syntax

```
icmp time-exceeded-packets
```

Mode

All Modes

Description

Generate ICMP time-exceeded packets.

Example

```
icmp time-exceeded-packets
```

Syntax

```
no icmp time-exceeded-packets
```

Mode

All Modes

Description

Never generate ICMP time-exceeded packets.

Example

```
no icmp time-exceeded-packets
```

Syntax

```
ftp-transforms-in-service-object { group <SVC_GROUP_NAME> | name <SVC_NAME> }
```

Mode

All Modes

Description

Enable FTP transformations for TCP port(s) in service object.

Options

<i>group</i>	Service group name.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<i><SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>

Example

ftp-transforms-in-service-object name Ping

Syntax

sqlnet

Mode

All Modes

Description

Enable support for oracle (SQLNet).

Example

sqlnet

Syntax

no sqlnet

Mode

All Modes

Description

Disable support for oracle (SQLNet).

Example

no sqlnet

Syntax

rtsp-transformations

Mode

All Modes

Description

Enable RTSP transformations.

Example

rtsp-transformations

Syntax

```
no rtsp-transformations
```

Mode

All Modes

Description

Disable RTSP transformations.

Example

```
no rtsp-transformations
```

Syntax

```
drop source-routed
```

Mode

All Modes

Description

Enable drop source routed IP packets.

Example

```
drop source-routed
```

Syntax

```
no drop source-routed
```

Mode

All Modes

Description

Disable drop source routed IP packets.

Example

```
no drop source-routed
```

Syntax

```
drop source-subnet-broadcast
```

Mode

All Modes

Description

Enable drop packets which source IP is subnet broadcast address.

Example

```
drop source-subnet-broadcast
```

Syntax

```
no drop source-subnet-broadcast
```

Mode

All Modes

Description

Disable drop packets which source IP is subnet broadcast address.

Example

```
no drop source-subnet-broadcast
```

Syntax

```
starting-vlan <UINT16>
```

Mode

All Modes

Description

Set starting VLAN ID.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
starting-vlan 2
```

Syntax

```
connections { highest | optimized | recommended }
```

Mode

All Modes

Description

Set the type of connections.

Options

highest UTM services (application firewall, anti-spyware, gateway AV, and IPS engine) disabled for highest number of SPI connections.

optimized Optimized for deployments requiring more UTM connections but less performance critical.

recommended Recommended for normal deployments with UTM services enabled.

Example

```
connections highest
```

Syntax

```
force-ftp-data
```

Mode

All Modes

Description

Force inbound and outbound FTP data connections to use the default port: 20.

Example

```
force-ftp-data
```

Syntax

```
no force-ftp-data
```

Mode

All Modes

Description

Disable force inbound and outbound FTP data connections to use the default port: 20.

Example

```
no force-ftp-data
```

Syntax

```
apply-rules-for-intra-lan
```

Mode

All Modes

Description

Enable apply firewall rules for intra-LAN traffic to/from the same interface.

Example

```
apply-rules-for-intra-lan
```

Syntax

```
no apply-rules-for-intra-lan
```

Mode

All Modes

Description

Disable apply firewall rules for intra-LAN traffic to/from the same interface.

Example

```
no apply-rules-for-intra-lan
```

Syntax

```
issue-rst-for-outgoing-discards
```

Mode

All Modes

Description

Enable always issue RST for discarded outgoing TCP connections.

Example

issue-rst-for-outgoing-discards

Syntax

no issue-rst-for-outgoing-discards

Mode

All Modes

Description

Disable always issue RST for discarded outgoing TCP connections.

Example

no issue-rst-for-outgoing-discards

Syntax

icmp redirect-on-lan

Mode

All Modes

Description

Enable ICMP redirect on LAN zone.

Example

icmp redirect-on-lan

Syntax

no icmp redirect-on-lan

Mode

All Modes

Description

Disable ICMP redirect on LAN zone.

Example

no icmp redirect-on-lan

Syntax

ip checksum-enforcement

Mode

All Modes

Description

Enable IP header checksum enforcement.

Example

ip checksum-enforcement

Syntax

no ip checksum-enforcement

Mode

All Modes

Description

Disable IP header checksum enforcement.

Example

no ip checksum-enforcement

Syntax

udp checksum-enforcement

Mode

All Modes

Description

Enable UDP checksum enforcement.

Example

udp checksum-enforcement

Syntax

no udp checksum-enforcement

Mode

All Modes

Description

Disable UDP checksum enforcement.

Example

no udp checksum-enforcement

Syntax

ipv6 drop { all-traffic | reserved-address-packets | routing-header-0 }

Mode

All Modes

Description

Configure firewall IPv6 drop actions.

Options

- all-traffic*** Enable drop all IPv6 traffic processing on this firewall.
- reserved-address-packets*** Enable drop and log network packets whose source or destination address is reserved by RFC.
- routing-header-0*** Enable drop IPv6 routing header type 0 packets.

Example

```
ipv6 drop all-ipv6-traffic
ipv6 drop routing-header-0
ipv6 drop reserved-address-packets
```

Syntax

```
no ipv6 drop { all-traffic | reserved-address-packets | routing-header-0 }
```

Mode

All Modes

Description

Configure firewall IPv6 drop actions.

Options

<i>all-traffic</i>	Disable drop all IPv6 traffic processing on this firewall.
<i>reserved-address-packets</i>	Disable drop and log network packets whose source or destination address is reserved by RFC.
<i>routing-header-0</i>	Disable drop IPv6 routing header type 0 packets.

Example

```
no ipv6 all-ipv6-traffic
no ipv6 drop routing-header-0
no ipv6 drop reserved-address-packets
```

Syntax

```
ipv6 decrement hop-limit
```

Mode

All Modes

Description

Enable decrement IPv6 hop limit for forwarded traffic.

Example

```
ipv6 decrement hop-limit
```

Syntax

```
no ipv6 decrement hop-limit
```

Mode

All Modes

Description

Disable decrement IPv6 hop limit for forwarded traffic.

Example

```
no ipv6 decrement hop-limit
```

Syntax

```
ipv6 icmp { destination-unreachable | parameter-problem | redirect | time-exceeded }
```

Mode

All Modes

Description

Set IPv6 ICMP packets.

Options

<i>destination-unreachable</i>	Generate IPv6 ICMP destination unreachable packets
<i>parameter-problem</i>	Generate IPv6 ICMP parameter problem packets
<i>redirect</i>	Generate IPv6 ICMP redirect packets
<i>time-exceeded</i>	Generate IPv6 ICMP time-exceeded packets

Example

```
ipv6 icmp time-exceeded
ipv6 icmp destination-unreachable
ipv6 icmp redirect
ipv6 icmp parameter-problem
```

Syntax

```
no ipv6 icmp { destination-unreachable | parameter-problem | redirect | time-exceeded }
```

Mode

All Modes

Description

Set IPv6 ICMP packets.

Options

<i>destination-unreachable</i>	Never generate IPv6 ICMP destination unreachable packets
<i>parameter-problem</i>	Never generate IPv6 ICMP parameter problem packets
<i>redirect</i>	Never generate IPv6 ICMP redirect packets
<i>time-exceeded</i>	Never generate IPv6 ICMP time-exceeded packets

Example

```
no ipv6 icmp time-exceeded
no ipv6 icmp destination-unreachable
no ipv6 icmp redirect
no ipv6 icmp parameter-problem
```

Syntax

```
ipv6 site-local-unicast
```

Mode

All Modes

Description

Enable allow to use site-local-unicast address.

Example

```
ipv6 site-local-unicast
```

Syntax

```
no ipv6 site-local-unicast
```

Mode

All Modes

Description

Disable allow to use site-local-unicast address.

Example

```
no ipv6 site-local-unicast
```

Syntax

```
ipv6 extension-header-check
```

Mode

All Modes

Description

Enable enforce IPv6 extension header validation.

Example

```
ipv6 extension-header-check
```

Syntax

```
no ipv6 extension-header-check
```

Mode

All Modes

Description

Disable enforce IPv6 extension header validation.

Example

```
no ipv6 extension-header-check
```

Syntax

```
ipv6 extension-header-order-check
```

Mode

All Modes

Description

Enable enforce IPv6 extension header order check.

Example

```
ipv6 extension-header-order-check
```

Syntax

```
no ipv6 extension-header-order-check
```

Mode

All Modes

Description

Disable enforce IPv6 extension header order check.

Example

```
no ipv6 extension-header-order-check
```

Syntax

```
ipv6 netbios-for-isatap
```

Mode

All Modes

Description

Enable NetBIOS name query response for ISATAP.

Example

```
ipv6 netbios-for-isatap
```

Syntax

```
no ipv6 netbios-for-isatap
```

Mode

All Modes

Description

Disable NetBIOS name query response for ISATAP.

Example

```
no ipv6 netbios-for-isatap
```

Syntax

```
control-plane-flood-protection
```

Mode

All Modes

Description

Enable control plane flood protection.

Example

```
control-plane-flood-protection
```

Syntax

```
no control-plane-flood-protection
```

Mode

All Modes

Description

Disable control plane flood protection.

Example

```
no control-plane-flood-protection
```

Syntax

```
control-plane-flood-protection-threshold <UINT8>
```

Mode

All Modes

Description

Set the control plane flood protection threshold (CPU %).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
control-plane-flood-protection threshold 75
```

Syntax

```
deregister firewall
```

Mode

Config

Description

deregistering the firewall.

Example

```
deregister firewall
```

Syntax

```
multicast
```

Mode

Config

Description

Enter multicast configuration mode.

Example

```
multicast
```

Syntax

enable

Mode

Multicast

Description

Enable multicast configuration.

Example

enable

Syntax

no enable

Mode

Multicast

Description

Disable multicast configuration.

Example

no enable

Syntax

enable-require-igmp-membership

Mode

Multicast

Description

Enable require IGMP membership reports for multicast data forwarding.

Example

enable-require-igmp-membership

Syntax

no enable-require-igmp-membership

Mode

Multicast

Description

Disable require IGMP membership reports for multicast data forwarding.

Example

no enable-require-igmp-membership

Syntax

require-igmp-membership-timeout <UINT8>

Mode

Multicast

Description

Multicast state table entry timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

require-igmp-membership

Syntax

no reception

Mode

Multicast

Description

Clear reception for the specified multicast addresses.

Example

no reception

Syntax

reception { all | group <MULTICAST_ADDR_GROUP_NAME> | host <MULTICAST_ADDR_HOST> | name <MULTICAST_ADDR_NAME> | network <MULTICAST_ADDR_NETWORK> <MULTICAST_ADDR_MASK> | range <MULTICAST_ADDR_BEGIN> <MULTICAST_ADDR_END> }

Mode

Multicast

Description

Enable reception for the specified multicast addresses.

Options

all	All multicast host.
group	Multicast address object group.
<MULTICAST_ADDR_GROUP_NAME>	Multicast address group name. Example: Multicast Group
host	Multicast address object host.
<MULTICAST_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n
name	Multicast address object name.
<MULTICAST_ADDR_NAME>	Multicast address object name. Example: Multicast Address
network	Multicast address object network.
<MULTICAST_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n
<MULTICAST_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: IPV4: 255.255.255.0\nIPV6: /64\n
range	Multicast address object range.

<MULTICAST_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<MULTICAST_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
reception all
reception name "Multicast Address"
reception group "Multicast Group"
reception host 224.0.0.12
reception range 192.168.168.10 192.168.168.20
reception network 192.168.168.0 255.255.255.0
```

Syntax

```
clear multicast state-entries
```

Mode

Multicast

Description

Clear all the IGMP state entries.

Example

```
clear multicast state-entries
```

Syntax

```
clear multicast state-entry address <MULTICAST_GROUP_IPV4_HOST> interface <MULTICAST_INTERFACE>
```

Mode

Multicast

Description

Clear the specified IGMP state entry.

Options

address	Specified multicast group address.
<MULTICAST_GROUP_IPV4_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
interface	Specified interface/ vpn tunnel.
<MULTICAST_INTERFACE>	Multicast interface name. Example: <i>X0</i>

Example

```
clear multicast state-entry address 2.2.2.2 interface X1
```

Syntax

```
no access-rule ipv4 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ]
```

Mode

Description

Delete firewall access rule policy.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object Group name. Example: <i>VOIP</i>
name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.

<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.

<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
no access-rule ipv4 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any
schedule name "After hours"
```

Syntax

```
clear access-rule statistics
```

Mode

Config

Description

Clear firewall access rule statistics.

Syntax

```
access-rule ipv4 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [
address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group
<SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any |
group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [
address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on
| days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ primitive ]
```

Mode

Config

Description

Add/edit firewall access rule and enter configuration mode.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>

host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com.

	Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
primitive	Configure a primitive access rule in one-line.

Example

```
access-rule ipv4 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any
schedule name "After hours"
```

Syntax

```
access-rule ipv4 uuid <UUID>
```

Mode

Config

Description

Edit firewall access rule by UUID and enter configuration mode.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36

Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
access-rule ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no access-rule ipv4 uuid <UUID>
```

Mode

Config

Description

Delete firewall access rule policy by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
no access-rule ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
access-rule restore-defaults [ from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> ]
```

Mode

Config

Description

Restore firewall access rules to default settings.

Options

from	From zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	To zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>

Example

```
access-rule restore-defaults from LAN to WAN
```

Syntax

```
access-rules max-count <UINT32>
```

Mode

Config

Description

Set max access rule count.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

access-rules max-count 800

Syntax

```
no access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] ] [ schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] ]
```

Mode

Config

Description

Delete firewall access rule policy.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>

range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.

<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
no access-rule ipv6 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any
schedule name "After hours"
```

Syntax

```
access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [
address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group
<SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any |
group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [
address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] } ] [ schedule { { always-on
| days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ primitive ]
```

Mode

Config

Description

Add/Edit firewall access rule and enter configuration mode.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination Zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.

fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH.

	Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
primitive	Configure a primitive IPv6 access rule in one-line.

Example

```
access-rule ipv6 from LAN to LAN action allow source address name "X0 IP" port any service name BGP destination address any
schedule name "After hours"
```

Syntax

```
no access-rule ipv6 uuid <UUID>
```

Mode

Config

Description

Delete firewall access rule policy by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

no access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

access-rule ipv6 uuid <UUID>

Mode

Config

Description

Edit firewall access rule by UUID and enter configuration mode.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

uuid <UUID>

Mode

Access Rule
Access Rule IPv6

Description

Access rule UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule UUID.

Example

```
no uuid
```

Syntax

```
name <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Access rule name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name OfficePolicy
```

Syntax

```
no name
```

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule name.

Example

```
no name
```

Syntax

```
from <ACCESS_RULE_ZONE_NAME>
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a source zone for this access rule.

Options

<ACCESS_RULE_ZONE_NAME> Access rule from.
Example: *DMZ*

Example

```
from LAN
```

Syntax

```
to <ACCESS_RULE_ZONE_NAME>
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a destination zone for this access rule.

Options

<ACCESS_RULE_ZONE_NAME> Access rule from.
Example: *DMZ*

Example

```
to LAN
```

Syntax

```
action { { allow | deny | discard } }
```

Mode

Access Rule
Access Rule IPv6

Description

Set the action for this access rule.

Options

allow Allow traffic matching the criteria.

deny Deny traffic matching the criteria.

discard Discard traffic matching the criteria.

Example

```
action allow
```

Syntax

```
max-connections <UINT8>
```

Mode

Access Rule
Access Rule IPv6

Description

Set the number of connections allowed (% maximum connections).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
max-connections 50
```

Syntax

```
priority { auto | end | manual <UINT32> }
```

Mode

Access Rule
Access Rule IPv6

Description

Set access rule priority.

Options

<i>auto</i>	Set auto priority(priority = 0) for access rule.
<i>end</i>	Insert the policy at the end.
<i>manual</i>	Set manual priority for access rule.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
priority auto
priority manual 1
```

Syntax

```
no priority manual
```

Mode

Access Rule
Access Rule IPv6

Description

Set access rule priority.

Options

<i>manual</i>	Set manual priority for access rule.

Example

```
no priority manual
```

Syntax

```
tcp timeout <UINT32>
```

Mode

Access Rule
Access Rule IPv6

Description

Set the TCP connection inactivity timeout (seconds).

Options

<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
tcp timeout 15
```

Syntax

udp timeout <UINT32>

Mode

Access Rule
Access Rule IPv6

Description

Set the UPD connection inactivity timeout (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

udp timeout 30

Syntax

fragments

Mode

Access Rule
Access Rule IPv6

Description

Allow fragmented packets on this access rule.

Example

fragments

Syntax

no fragments

Mode

Access Rule
Access Rule IPv6

Description

Disable fragmented packets on this access rule.

Example

no fragments

Syntax

botnet-filter

Mode

Access Rule
Access Rule IPv6

Description

Enable Botnet filter.

Example

```
botnet-filter
```

Syntax

```
no botnet-filter
```

Mode

Access Rule
Access Rule IPv6

Description

Disable Botnet filter.

Example

```
no botnet-filter
```

Syntax

```
comment <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a comment for this access rule.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Access Rule to allow IT to access servers"
```

Syntax

```
no comment
```

Mode

Access Rule
Access Rule IPv6

Description

Clear a comment for this access rule.

Example

```
no comment
```

Syntax

```
connection-limit destination [ threshold <UINT16> ]
```

Mode

Access Rule
Access Rule IPv6

Description

Enable connection limit for each destination IP address.

Options

- threshold*** Set the destination IP address connection limit threshold.
- <UINT16>*** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
connection-limit destination threshold 128
```

Syntax

```
no connection-limit destination [ threshold ]
```

Mode

Access Rule
Access Rule IPv6

Description

Disable connection limit for each destination IP address.

Options

- threshold*** Clear the destination IP address connection limit threshold.

Example

```
no connection-limit destination
```

Syntax

```
connection-limit source [ threshold <UINT16> ]
```

Mode

Access Rule
Access Rule IPv6

Description

Enable connection limit for each source IP address.

Options

- threshold*** Set the source IP address connection limit threshold.
- <UINT16>*** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
connection-limit source threshold 128
```

Syntax

```
no connection-limit source [ threshold ]
```

Mode

Access Rule
Access Rule IPv6

Description

Disable connection limit for each source IP address.

Options

threshold Clear the source IP address connection limit threshold.

Example

```
no connection-limit source
```

Syntax

```
tcp urgent
```

Mode

Access Rule
Access Rule IPv6

Description

Enable allow TCP urgent packets.

Example

```
tcp-urgent
```

Syntax

```
no tcp urgent
```

Mode

Access Rule
Access Rule IPv6

Description

Disable allow TCP urgent packets.

Example

```
no tcp urgent
```

Syntax

```
dpi
```

Mode

Access Rule
Access Rule IPv6

Description

Enable DPI.

Example

```
dpi
```

Syntax

```
no dpi
```

Mode

Access Rule
Access Rule IPv6

Description

Disable DPI.

Example

```
no dpi
```

Syntax

```
dpi-ssl { client | server }
```

Mode

Access Rule
Access Rule IPv6

Description

Enable DPI-SSL client or server.

Options

client Enable DPI-SSL client.

server Enable DPI-SSL server.

Example

```
dpi-ssl client  
dpi-ssl server
```

Syntax

```
no dpi-ssl { client | server }
```

Mode

Access Rule
Access Rule IPv6

Description

Disable DPI-SSL client or server.

Options

client Disable DPI-SSL client.

server Disable DPI-SSL server.

Example

```
no dpi-ssl client  
no dpi-ssl server
```

Syntax

```
redirect-unauthenticated-users-to-log-in
```

Mode

Description

Enable redirect unauthenticated users to log in.

Example

redirect-unauthenticated-users-to-log-in

Syntax

no redirect-unauthenticated-users-to-log-in

Mode

Description

Disable redirect unauthenticated users to log in.

Example

no redirect-unauthenticated-users-to-log-in

Syntax

destination address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }

Mode

Description

Specify a destination for this access rule.

Options

<i>any</i>	Any address.
<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_GROUP_NAME_WITH_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>mac</i> <ADDR_MAC>	Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i> <ADDR_NAME_WITH_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
<i>network</i> <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>

<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
destination address name "Corporate Servers"
```

Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a service for this Access Policy.

Options

any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
service "Corporate Servers"
```

Syntax

```
enable
```

Mode

Access Rule
Access Rule IPv6

Description

Enable this access rule.

Example

```
enable
```

Syntax

no enable

Mode

Access Rule
Access Rule IPv6

Description

Disable this access rule.

Example

no enable

Syntax

auto-rule

Mode

Access Rule
Access Rule IPv6

Description

Indicate it is an auto rule.

Example

auto-rule

Syntax

no auto-rule

Mode

Access Rule
Access Rule IPv6

Description

Indicate it is an auto rule.

Example

no auto-rule

Syntax

flow-reporting

Mode

Access Rule
Access Rule IPv6

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Access Rule
Access Rule IPv6

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

geo-ip-filter { custom | enable | global }

Mode

Access Rule
Access Rule IPv6

Description

Enable Geo-IP filter.

Options

custom Enable Geo-IP filter global mode.

enable Enable Geo-IP filter.

global Enable Geo-IP filter global mode.

Example

geo-ip-filter

Syntax

no geo-ip-filter enable

Mode

Access Rule
Access Rule IPv6

Description

Disable Geo-IP filter.

Options

enable Enable Geo-IP filter.

Example

no geo-ip-filter

Syntax


```
block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Access Rule
Access Rule IPv6

Description

Set blocked country from the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
block country Antartica
```

Syntax

```
no block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Access Rule
Access Rule IPv6

Description

Disable the country in the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
no block country Canada
```

Syntax

```
block countries [ unknown ]
```

Mode

Access Rule
Access Rule IPv6

Description

Set block countries for Geo-IP.

Options

unknown Enable block all unknown countries.

Example

```
block countries  
block countries unknown
```

Syntax

```
no block countries [ unknown ]
```

Mode

Access Rule
Access Rule IPv6

Description

Set block countries for Geo-IP.

Options

unknown Disable block all unknown countries.

Example

```
no block countries
no block countries unknown
```

Syntax

logging

Mode

Access Rule
Access Rule IPv6

Description

Enable logging when this access rule is used.

Example

```
logging
```

Syntax

no logging

Mode

Access Rule
Access Rule IPv6

Description

Disable logging when this access rule is used.

Example

```
no logging
```

Syntax

sip

Mode

Access Rule
Access Rule IPv6

Description

Enable SIP transformation.

Example

```
sip
```

Syntax

no sip

Mode

Access Rule
Access Rule IPv6

Description

Disable SIP transformation.

Example

no sip

Syntax

h323

Mode

Access Rule
Access Rule IPv6

Description

Enable H.323 transformation.

Example

h323

Syntax

no h323

Mode

Access Rule
Access Rule IPv6

Description

Disable H.323 transformation.

Example

no h323

Syntax

packet-monitoring

Mode

Access Rule
Access Rule IPv6

Description

Enable packet monitoring.

Example

packet-monitoring

Syntax

no packet-monitoring

Mode

Access Rule
Access Rule IPv6

Description

Disable packet monitoring.

Example

no packet-monitoring

Syntax

packet-dissection-filter { { group <PDF_GROUP_NAME> | name <PDF_NAME> } }

Mode

Access Rule
Access Rule IPv6

Description

Add packet dissection filter.

Options

- group** Packer dissection filter group name.
- <PDF_GROUP_NAME>** Packet Dissection Group name.
Example: PdfGroupName
- name** Packer dissection filter object name.
- <PDF_NAME>** Packet Dissection object name.
Example: PdfName

Example

packet-dissection-filter "Corp Address"

Syntax

no packet-dissection-filter

Mode

Access Rule
Access Rule IPv6

Description

Clear packet dissection filter.

Example

no packet-dissection-filter

Syntax

management

Mode

Access Rule
Access Rule IPv6

Description

Allow management traffic.

Example

```
management
```

Syntax

```
no management
```

Mode

Access Rule
Access Rule IPv6

Description

Disable management traffic.

Example

```
no management
```

Syntax

```
single-sign-on
```

Mode

Access Rule
Access Rule IPv6

Description

Invoke single sign on to authenticate users.

Example

```
single-sign-on
```

Syntax

```
no single-sign-on
```

Mode

Access Rule
Access Rule IPv6

Description

Don't invoke single sign on to authenticate users.

Example

```
no single-sign-on
```

Syntax

```
block-traffic-for-single-sign-on
```

Mode

Access Rule

Description

Block traffic while waiting for Single Sign On to authenticate users.

Example

```
block-traffic-for-single-sign-on
```

Syntax

```
no block-traffic-for-single-sign-on
```

Mode

Access Rule

Description

Don't block traffic while waiting for Single Sign On to authenticate users.

Example

```
no block-traffic-for-single-sign-on
```

Syntax

```
quality-of-service class-of-service { explicit { { background | best-effort | controlled-load | excellent-effort | network-control | spare | video | voice } } | map | preserve }
```

Mode

Access Rule

Access Rule IPv6

Description

Set 802.1p marking action.

Options

<i>explicit</i>	Set explicit marking.
<i>background</i>	Background.
<i>best-effort</i>	Best effort.
<i>controlled-load</i>	Controlled load.
<i>excellent-effort</i>	Excellent effort.
<i>network-control</i>	Network control.
<i>spare</i>	Spare.
<i>video</i>	Video (<100ms latency).
<i>voice</i>	Voice (<10ms latency).
<i>map</i>	Map marking.
<i>preserve</i>	Preserve marking.

Example

```
quality-of-service class-of-service preserve
```

Syntax

cos-override

Mode

Access Rule
Access Rule IPv6

Description

Allow 802.1p marking to override DSCP values.

Example

cos-override

Syntax

no cos-override

Mode

Access Rule
Access Rule IPv6

Description

Disable allowing 802.1p marking to override DSCP values.

Example

no cos-override

Syntax

no quality-of-service { class-of-service | dscp [explicit] }

Mode

Access Rule
Access Rule IPv6

Description

Clear DSCP and 802.1p marking settings.

Options

<i>class-of-service</i>	No 802.1p tagging.
<i>dscp</i>	Clear DSCP values.
<i>explicit</i>	Clear explicit marking value.

Example

no quality-of-service dscp

Syntax

quality-of-service dscp { explicit <UINT8> | map | preserve }

Mode

Access Rule
Access Rule IPv6

Description

Set DSCP marking action.

Options

explicit Set explicit marking.
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

map Map marking.

preserve Preserve marking.

Example

quality-of-service dscp preserve

Syntax

reflexive

Mode

Access Rule
Access Rule IPv6

Description

Configure a reflexive rule.

Example

reflexive

Syntax

no reflexive

Mode

Access Rule
Access Rule IPv6

Description

Disable configuration of a reflexive rule.

Example

no reflexive

Syntax

schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } }

Mode

Access Rule
Access Rule IPv6

Description

Specify a schedule for this access rule.

Options

always-on Always on.

days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule name "IT Maintenance"
```

Syntax

```
source address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a service for this access rule.

Options

any	Any address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_WITH_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_WITH_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

```
source address name "Corporate IT Administration"
```

Syntax

```
source port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify a source port for this access rule.

Options

any	Any source service.
group	Source service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Source service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
source port name "Corporate IT Administration"
```

Syntax

```
users included { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> } }
```

Mode

Access Rule
Access Rule IPv6

Description

Specify users that apply to this access rule.

Options

administrator	Administrator.
all	All users.
group	Group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guest users.
name	User object name.

<LOCAL_USER_NAME> Local user object name.
Example: *user1*

Example

users included name "Corporate IT Administrators"

Syntax

users excluded { { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> | none } }

Mode

Access Rule
Access Rule IPv6

Description

Specify users that are excluded from this access rule.

Options

- administrator** Administrator.
- group** Group object name.
<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*
- guests** Guest users.
- name** User object name.
<LOCAL_USER_NAME> Local user object name.
Example: *user1*
- none** No users.

Example

users excluded name "Corporate Users"

Syntax

bandwidth-management

Mode

Access Rule

Description

Enter ethernet bandwidth management configuration mode.

Example

bandwidth-management

Syntax

bandwidth-management

Mode

Access Rule IPv6

Description

Enter bandwidth management configuration mode.

Example

```
bandwidth-management
```

Syntax

```
egress { bandwidth-object <BANDWIDTH_RULE_NAME> }
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable egress bandwidth management and configure.

Options

<i>bandwidth-object</i>	Bandwidth object name.
<i><BANDWIDTH_RULE_NAME></i>	Bandwidth object name. Example: <code>\ "Corp High Priority\"</code>

Example

```
egress bandwidth-object "Corp High Priority"
```

Syntax

```
no egress
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable egress bandwidth management.

Example

```
no egress
```

Syntax

```
ingress { bandwidth-object <BANDWIDTH_RULE_NAME> }
```

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable ingress bandwidth management and configure.

Options

<i>bandwidth-object</i>	Bandwidth object name.
<i><BANDWIDTH_RULE_NAME></i>	Bandwidth object name. Example: <code>\ "Corp High Priority\"</code>

Example

```
ingress bandwidth-object "Corp High Priority"
```

Syntax

no ingress

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable ingress bandwidth management.

Example

no ingress

Syntax

usage-tracking

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Enable tracking bandwidth usage.

Example

usage-tracking

Syntax

no usage-tracking

Mode

Bandwidth Management
Bandwidth Management IPv6

Description

Disable tracking bandwidth usage.

Example

no usage-tracking

Syntax

ticket tag1 <WORD>

Mode

Access Rule
Access Rule IPv6

Description

Set access rule ticket tag 1.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag1 "Tag number 1"
```

Syntax

```
no ticket tag1
```

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule ticket tag 1.

Example

```
no ticket tag1
```

Syntax

```
ticket tag2 <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Set access rule ticket tag 2.

Options

<**WORD**> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag2 "Tag number 2"
```

Syntax

```
no ticket tag2
```

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule ticket tag 2.

Example

```
no ticket tag2
```

Syntax

```
ticket tag3 <WORD>
```

Mode

Access Rule
Access Rule IPv6

Description

Set access rule ticket tag 3.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ticket tag3 "Tag number 3"

Syntax

no ticket tag3

Mode

Access Rule
Access Rule IPv6

Description

Clear access rule ticket tag 3.

Example

no ticket tag3

Syntax

clear policy lookup

Mode

Config

Description

Reset the values to the default policy lookup settings.

Options

lookup lookup settings

Example

clear policy lookup

Syntax

generate shadow-list { access-rules | decryption-policies | dos-policies | nat-policies | route-policies }

Mode

Config

Description

Generate Shadow Rule List.

Options

access-rules Generate shadow access-rules list.

decryption-policies Generate shadow decryption-policies list.

<i>dos-policies</i>	Generate shadow dos-policies list.
<i>nat-policies</i>	Generate shadow nat-policies list.
<i>route-policies</i>	Generate shadow route-policies list.

Example

```
generate shadow-list access-rules
```

Syntax

```
ssl-control
```

Mode

Config

Description

Enter SSL control mode and configure settings.

Example

```
ssl-control
```

Syntax

```
enable
```

Mode

SSL Control

Description

Enable SSL control.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SSL Control

Description

Disable SSL control.

Example

```
no enable
```

Syntax

```
action { block | log }
```

Mode

SSL Control

Description

Action if an SSL policy violation is detected.

Options

block Block the connection and log the event.

log Log the event.

Example

```
action block
```

Syntax

```
blacklist
```

Mode

SSL Control

Description

Enable blacklist.

Example

```
blacklist
```

Syntax

```
no blacklist
```

Mode

SSL Control

Description

Disable blacklist.

Example

```
no blacklist
```

Syntax

```
detect ssl-v2
```

Mode

SSL Control

Description

Enable detection of SSLv2.

Example

```
detect ssl-v2
```

Syntax

```
no detect ssl-v2
```

Mode

SSL Control

Description

Disable detection of SSLv2.

Example

```
no detect ssl-v2
```

Syntax

```
detect ssl-v3
```

Mode

SSL Control

Description

Enable detection of SSLv3.

Example

```
detect ssl-v3
```

Syntax

```
no detect ssl-v3
```

Mode

SSL Control

Description

Disable detection of SSLv3.

Example

```
no detect ssl-v3
```

Syntax

```
detect weak-ciphers
```

Mode

SSL Control

Description

Enable detection of weak ciphers.

Example

```
detect weak-ciphers
```

Syntax

```
no detect weak-ciphers
```

Mode

SSL Control

Description

Disable detection of weak ciphers.

Example

```
no detect weak-ciphers
```

Syntax

```
whitelist
```

Mode

SSL Control

Description

Enable whitelist.

Example

```
whitelist
```

Syntax

```
no whitelist
```

Mode

SSL Control

Description

Disable whitelist.

Example

```
no whitelist
```

Syntax

```
detect self-signed
```

Mode

SSL Control

Description

Enable detection of self-signed certificates.

Example

```
detect self-signed
```

Syntax

```
no detect self-signed
```

Mode

SSL Control

Description

Disable detection of self-signed certificates.

Example

```
no detect self-signed
```

Syntax

```
detect weak-digest-cert
```

Mode

SSL Control

Description

Enable detection of weak digest certificates.

Example

```
detect weak-digest-cert
```

Syntax

```
no detect weak-digest-cert
```

Mode

SSL Control

Description

Disable detection of weak digest certificates.

Example

```
no detect weak-digest-cert
```

Syntax

```
detect expired
```

Mode

SSL Control

Description

Enable detection of expired certificates.

Example

```
detect expired
```

Syntax

```
no detect expired
```

Mode

SSL Control

Description

Disable detection of expired certificates.

Example

```
no detect expired
```

Syntax

detect untrusted-ca

Mode

SSL Control

Description

Enable detection of certificate signed by an untrusted CA.

Example

detect untrusted-ca

Syntax

no detect untrusted-ca

Mode

SSL Control

Description

Disable detection of certificate signed by an untrusted CA.

Example

no detect untrusted-ca

Syntax

detect tls-v1

Mode

SSL Control

Description

Enable detection of TLSv1.

Example

detect tls-v1

Syntax

no detect tls-v1

Mode

SSL Control

Description

Disable detection of TLSv1.

Example

no detect tls-v1

Syntax

```
blacklist-certificate <BLACKLIST_CERTIFICATE>
```

Mode

SSL Control

Description

Add/edit blacklist entry and enter to its sub-mode.

Options

<BLACKLIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

```
blacklist-certificate www.badguys.com
```

Syntax

```
no blacklist-certificate <BLACKLIST_CERTIFICATE>
```

Mode

SSL Control

Description

Delete an entry from blacklist.

Options

<BLACKLIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

```
no blacklist-certificate www.badguys.com
```

Syntax

```
no blacklist-certificates
```

Mode

SSL Control

Description

Delete all entries from blacklist.

Example

```
no blacklist-certificates
```

Syntax

```
common-name <WORD>
```

Mode

SSL Control Black Lists

Description

Common name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

common-name www.badguys2.com

Syntax

whitelist-certificate <WHITELIST_CERTIFICATE>

Mode

SSL Control

Description

Add/edit whitelist entry and enter to its sub-mode.

Options

<WHITELIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

whitelist-certificate www.badguys.com

Syntax

no whitelist-certificate <WHITELIST_CERTIFICATE>

Mode

SSL Control

Description

Delete an entry from whitelist.

Options

<WHITELIST_CERTIFICATE> Word in the form: WORD or \"QUOTED STRING\".
Example: *certificateName*

Example

no whitelist-certificate www.goodguys.com

Syntax

no whitelist-certificates

Mode

SSL Control

Description

Delete all entries from whitelist.

Example

no whitelist-certificates

Syntax

common-name <WORD>

Mode

SSL Control White Lists

Description

Common name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

common-name *www.goodguys2.com*

Syntax

tcp

Mode

Config

Description

Configure TCP settings.

Example

tcp

Syntax

enforce-strict-compliance

Mode

TCP

Description

Enable enforcement of strict TCP compliance with RFC 793 and RFC 1122.

Example

enforce-strict-compliance

Syntax

no enforce-strict-compliance

Mode

TCP

Description

Disable enforcement of strict TCP compliance with RFC 793 and RFC 1122.

Example

no enforce-strict-compliance

Syntax

handshake-enforcement

Mode

TCP

Description

Enable TCP handshake enforcement.

Example

handshake-enforcement

Syntax

no handshake-enforcement

Mode

TCP

Description

Disable TCP handshake enforcement.

Example

no handshake-enforcement

Syntax

checksum-enforcement

Mode

TCP

Description

Enable TCP checksum enforcement.

Example

checksum-enforcement

Syntax

no checksum-enforcement

Mode

TCP

Description

Disable TCP checksum enforcement.

Example

no checksum-enforcement

Syntax

drop syn-with-data

Mode

TCP

Description

Enable drop TCP SYN with data packets.

Example

```
drop syn-with-data
```

Syntax

```
no drop syn-with-data
```

Mode

TCP

Description

Disable drop TCP SYN with data packets.

Example

```
no drop syn-with-data
```

Syntax

```
drop invalid-urgent
```

Mode

TCP

Description

Enable drop invalid TCP urgent packets.

Example

```
drop invalid-urgent
```

Syntax

```
no drop invalid-urgent
```

Mode

TCP

Description

Disable drop invalid TCP urgent packets.

Example

```
no drop invalid-urgent
```

Syntax

```
enable-handshake-timeout
```

Mode

TCP

Description

Enable the TCP handshake timeout configure.

Example

```
enable handshake-timeout 4
```

Syntax

```
no enable-handshake-timeout
```

Mode

TCP

Description

Disable the TCP handshake timeout configure.

Example

```
no enable handshake-timeout
```

Syntax

```
handshake-timeout <UINT32>
```

Mode

TCP

Description

Set the TCP handshake timeout in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
handshake-timeout 4
```

Syntax

```
default-connection-timeout <UINT32>
```

Mode

TCP

Description

Set default TCP connection timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
default-connection-timeout 15
```

Syntax

maximum-segment-lifetime <UINT8>

Mode

TCP

Description

Set maximum segment lifetime in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

maximum-segment-lifetime 8

Syntax

half-open-threshold

Mode

TCP

Description

Enable half open TCP connections threshold.

Example

half-open-threshold

Syntax

no half-open-threshold

Mode

TCP

Description

Disable half open TCP connections threshold.

Example

no half-open-threshold

Syntax

maximum-half-open-connections <UINT32>

Mode

TCP

Description

Set maximum half open TCP connections.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
maximum-half-open-connections 562496
```

Syntax

```
syn-flood-protection-mode { always-proxy | proxy-suspect-attack | watch-and-report }
```

Mode

TCP

Description

Set TCP SYN flood protection mode.

Options

always-proxy Always proxy WAN client connections.

proxy-suspect-attack Proxy WAN client connections when attack is suspected.

watch-and-report Watch and report possible SYN floods.

Example

```
syn-flood-protection-mode watch-and-report
```

Syntax

```
syn-attack-threshold <UINT32>
```

Mode

TCP

Description

Set attack threshold (incomplete connection attempts / second).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
syn-attack-threshold 300
```

Syntax

```
support-tcp-sack
```

Mode

TCP

Description

Enable all LAN/DMZ servers support the TCP SACK option.

Example

```
support-tcp-sack
```

Syntax

```
no support-tcp-sack
```

Mode

TCP

Description

Disable all LAN/DMZ servers support the TCP SACK option.

Example

```
no support-tcp-sack
```

Syntax

```
enable-limit-mss
```

Mode

TCP

Description

Enable limit MSS sent to WAN clients (when connections are proxied).

Example

```
enable-limit-mss
```

Syntax

```
no enable-limit-mss
```

Mode

TCP

Description

Disable limit MSS sent to WAN clients (when connections are proxied).

Example

```
no enable-limit-mss
```

Syntax

```
limit-mss-max <UINT16>
```

Mode

TCP

Description

Set the maximum TCP MSS sent to WAN clients.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
limit-mss-max 1460
```

Syntax

always-log-syn-packets

Mode

TCP

Description

Enable always log SYN packets received.

Example

always-log-syn-packets

Syntax

no always-log-syn-packets

Mode

TCP

Description

Disable always log SYN packets received.

Example

no always-log-syn-packets

Syntax

proxy-connections [service { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }]

Mode

TCP

Description

Enable proxy connections for specific service only and select the specific service.

Options

<i>service</i>	Set the specific service.
<i>any</i>	Any service.
<i>group</i>	Service group name.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<i><SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>
<i>protocol</i>	Service object protocol.
<i><SVC_PROTOCOL></i>	Service protocol. Example: <i>TCP</i>
<i><SVC_PORT_BEGIN></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i><SVC_PORT_END></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

proxy-connections
proxy-connections service any
proxy-connections service name HTTP

Syntax

no proxy-connections

Mode

TCP

Description

Disable proxy connections for specific service only.

Example

no proxy-connections

Syntax

syn-flood-blacklisting

Mode

TCP

Description

Enable SYN/RST/FIN flood blacklisting on all interfaces.

Example

syn-flood-blacklisting

Syntax

no syn-flood-blacklisting

Mode

TCP

Description

Disable SYN/RST/FIN flood blacklisting on all interfaces.

Example

no syn-flood-blacklisting

Syntax

blacklist-threshold <UINT32>

Mode

TCP

Description

Set threshold for SYN/RST/FIN flood blacklisting (packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
blacklist-threshold 1000
```

Syntax

```
never-blacklist-wan
```

Mode

TCP

Description

Enable never blacklist WAN machines.

Example

```
never-blacklist-wan
```

Syntax

```
no never-blacklist-wan
```

Mode

TCP

Description

Disable never blacklist WAN machines.

Example

```
no never-blacklist-wan
```

Syntax

```
always-allow-management
```

Mode

TCP

Description

Enable always allow SonicWall management traffic.

Example

```
always-allow-management
```

Syntax

```
no always-allow-management
```

Mode

TCP

Description

Disable always allow SonicWall management traffic.

Example

```
no always-allow-management
```

Syntax

ddos on-wan-interfaces

Mode

TCP

Description

Enable DDOS protection on WAN interfaces.

Example

ddos on-wan-interfaces

Syntax

no ddos on-wan-interfaces

Mode

TCP

Description

Disable DDOS protection on WAN interfaces.

Example

no ddos on-wan-interfaces

Syntax

ddos threshold <UINT32>

Mode

TCP

Description

Set threshold for WAN DDOS protection (non-TCP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

ddos threshold 1000

Syntax

no ddos threshold

Mode

TCP

Description

Clear threshold for WAN DDOS protection.

Example

no ddos threshold

Syntax

ddos fliter-bypass-rate <UINT32>

Mode

TCP

Description

Set WAN DDOS filter bypass rate (every n packets).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

ddos fliter-bypass-rate 100

Syntax

no ddos fliter-bypass-rate

Mode

TCP

Description

Clear WAN DDOS filter bypass rate.

Example

no ddos fliter-bypass-rate

Syntax

ddos allow-list-timeout <UINT32>

Mode

TCP

Description

Set WAN DDOS allow list timeout.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

ddos allow-list-timeout 100

Syntax

no ddos allow-list-timeout

Mode

TCP

Description

Clear WAN DDOS allow list timeout.

Example

```
no ddos allow-list-timeout
```

Syntax

```
ddos always-allow-management
```

Mode

TCP

Description

Enable always allow SonicWall management traffic (non-tcp floods).

Example

```
ddos always-allow-management
```

Syntax

```
no ddos always-allow-management
```

Mode

TCP

Description

Disable always allow SonicWall management traffic (non-tcp floods).

Example

```
no ddos always-allow-management
```

Syntax

```
ddos always-allow-negotiation
```

Mode

TCP

Description

Enable always allow VPN negotiation traffic (non-tcp floods).

Example

```
ddos always-allow-negotiation
```

Syntax

```
no ddos always-allow-negotiation
```

Mode

TCP

Description

Disable always allow VPN negotiation traffic (non-tcp floods).

Example

```
no ddos always-allow-negotiation
```

Syntax

```
clear tcp statistics
```

Mode

TCP

Description

Clear TCP traffic statistics.

Example

```
clear tcp statistics
```

Syntax

```
no bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Config

Description

Delete a bandwidth object.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\ "Corp High Priority\"`

Example

```
no bandwidth-object "Corp High Priority"
```

Syntax

```
no bandwidth-objects
```

Mode

Config

Description

Delete all custom bandwidth objects.

Example

```
no bandwidth-objects
```

Syntax

```
bandwidth-object <BANDWIDTH_OBJ_NAME>
```

Mode

Config

Description

Add/edit a bandwidth object and enter its configuration mode.

Options

<BANDWIDTH_OBJ_NAME> Bandwidth object name.
Example: `\ "Corp High Priority\"`

Example

`bandwidth-object "Corp High Priority"`

Syntax

`name <BANDWIDTH_OBJ_NAME>`

Mode

Bandwidth Object

Description

Set bandwidth object name.

Options

<BANDWIDTH_OBJ_NAME> Bandwidth object name.
Example: `\ "Corp High Priority\"`

Example

`name "Corp High Priority"`

Syntax

`guaranteed { kbps <UINT64> | mbps <UINT64> }`

Mode

Bandwidth Object

Description

Set bandwidth object guaranteed bandwidth.

Options

kbps Kilobits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: `123`

mbps Megabits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: `123`

Example

`guaranteed mbps 50`

Syntax

`no guaranteed { kbps | mbps }`

Mode

Bandwidth Object

Description

Clear bandwidth object guaranteed bandwidth.

Options

- kbps*** Kilobits per second.
- mbps*** Megabits per second.

Example

no guaranteed kbps

Syntax

maximum { kbps <UINT64> | mbps <UINT64> }

Mode

Bandwidth Object

Description

Set bandwidth object maximum bandwidth.

Options

- kbps*** Kilobits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: *123*
- mbps*** Megabits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: *123*

Example

maximum mbps 100

Syntax

priority { high | highest | low | lowest | medium | medium-high | medium-low | realtime }

Mode

Bandwidth Object

Description

Set the bandwidth object traffic priority.

Options

- high*** High 2.
- highest*** Highest 1.
- low*** Low 6.
- lowest*** Lowest 7.
- medium*** Medium 4.
- medium-high*** Medium-high 3.

medium-low Medium-low 5.

realtime Realtime 0.

Example

priority medium-high

Syntax

action { delay | drop }

Mode

Bandwidth Object

Description

Set the bandwidth object violation action.

Options

delay Delay.

drop Drop.

Example

action delay

Syntax

comment <WORD>

Mode

Bandwidth Object

Description

Set comment for the bandwidth object.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Use to insure maximum bandwidth for high priority traffic"

Syntax

no comment

Mode

Bandwidth Object

Description

Clear a comment for the bandwidth object.

Example

no comment

Syntax

```
per-ip-management { kbps <UINT64> | mbps <UINT64> }
```

Mode

Bandwidth Object

Description

Enable per IP bandwidth management and set the maximum bandwidth.

Options

kbps Kilobits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: *123*

mbps Megabits per second.
<UINT64> Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH.
Example: *123*

Example

```
per-ip-management kbps 800
```

Syntax

```
no per-ip-management
```

Mode

Bandwidth Object

Description

Disable per IP bandwidth management.

Example

```
no per-ip-management
```

Syntax

```
cipher-control tls
```

Mode

Config

Description

Configure cipher control TLS settings.

Example

```
cipher-control tls
```

Syntax

```
cipher-control ssh
```

Mode

Config

Description

Configure cipher control SSH settings.

Example

```
cipher-control ssh
```

Syntax

```
no cipher <CIPHER_CONTROL_CIPHERS>
```

Mode

Cipher Control TLS

Description

Block tls cipher.

Options

<CIPHER_CONTROL_CIPHERS> Cipher control block ciphers.
Example: *TLS_AES_128_GCM_SHA256*

Example

```
no cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

Syntax

```
cipher <CIPHER_CONTROL_CIPHERS>
```

Mode

Cipher Control TLS

Description

Unblock tls cipher.

Options

<CIPHER_CONTROL_CIPHERS> Cipher control block ciphers.
Example: *TLS_AES_128_GCM_SHA256*

Example

```
cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

Syntax

```
no ciphers strength { all | insecure | recommended | secure | weak } action { all | allow | block } cbc { all | is | not } [ tls10 ] [ tls11 ] [ tls12 ] [ tls13 ]
```

Mode

Cipher Control TLS

Description

Block tls ciphers.

Options

all Ciphers of all strengths .

insecure Ciphers of insecure strength.

<i>recommended</i>	Ciphers of recommended strength.
<i>secure</i>	Ciphers of secure strength.
<i>weak</i>	Ciphers of weak strength.
<i>action</i>	Cipher current action.
<i>all</i>	Ciphers that are currently set to blocked or unblocked.
<i>allow</i>	Ciphers that are currently set to unblocked.
<i>block</i>	Ciphers that are currently set to blocked.
<i>cbc</i>	Cipher CBC status.
<i>all</i>	Ciphers that do and don't use block chaining.
<i>is</i>	Ciphers that use block chaining.
<i>not</i>	Ciphers that don't use block chaining.
<i>tls10</i>	Include TLS1.0 Ciphers.
<i>tls11</i>	Include TLS1.1 Ciphers.
<i>tls12</i>	Include TLS1.2 Ciphers.
<i>tls13</i>	Include TLS1.3 Ciphers.

Example

```
no ciphers strength weak action allow cbc all tls1.0 tls1.1 tls1.2 tls1.3
```

Syntax

```
ciphers strength { all | insecure | recommended | secure | weak } action { all | allow | block } cbc { all | is | not } [
tls10 ] [ tls11 ] [ tls12 ] [ tls13 ]
```

Mode

Cipher Control TLS

Description

Unblock TLS ciphers.

Options

<i>all</i>	Ciphers of all strengths.
<i>insecure</i>	Ciphers of insecure strength.
<i>recommended</i>	Ciphers of recommended strength.
<i>secure</i>	Ciphers of secure strength.
<i>weak</i>	Ciphers of weak strength.
<i>action</i>	Cipher current action.
<i>all</i>	Ciphers that are currently set to blocked or unblocked.
<i>allow</i>	Ciphers that are currently set to unblocked.
<i>block</i>	Ciphers that are currently set to blocked.
<i>cbc</i>	Cipher CBC status.
<i>all</i>	Ciphers that do and don't use block chaining.
<i>is</i>	Ciphers that use block chaining.
<i>not</i>	Ciphers that don't use block chaining.

<i>tls10</i>	Include TLS1.0 Ciphers.
<i>tls11</i>	Include TLS1.1 Ciphers.
<i>tls12</i>	Include TLS1.2 Ciphers.
<i>tls13</i>	Include TLS1.3 Ciphers.

Example

```

ciphers strength recommended action all cbc all tls1.2

```

Syntax

```

no key-exchange { diffie-hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha256 | diffie-hellman-group1-sha1 |
diffie-hellman-group14-sha1 }

```

Mode

Cipher Control SSH

Description

Disable ssh key exchange algorithm.

Options

<i>diffie-hellman-group-exchange-sha1</i>	Diffie-hellman-group-exchange-sha1.
<i>diffie-hellman-group-exchange-sha256</i>	Diffie-hellman-group-exchange-sha256.
<i>diffie-hellman-group1-sha1</i>	Diffie-hellman-group1-sha1.
<i>diffie-hellman-group14-sha1</i>	Diffie-hellman-group14-sha1.

Example

```

no key-exchange diffie-hellman-group1-sha1

```

Syntax

```

key-exchange { diffie-hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha256 | diffie-hellman-group1-sha1 |
diffie-hellman-group14-sha1 }

```

Mode

Cipher Control SSH

Description

Enable ssh key exchange algorithm.

Options

<i>diffie-hellman-group-exchange-sha1</i>	Diffie-hellman-group-exchange-sha1.
<i>diffie-hellman-group-exchange-sha256</i>	Diffie-hellman-group-exchange-sha256.
<i>diffie-hellman-group1-sha1</i>	Diffie-hellman-group1-sha1.
<i>diffie-hellman-group14-sha1</i>	Diffie-hellman-group14-sha1.

Example

```

key-exchange diffie-hellman-group1-sha1

```

Syntax

```
no public-key { rsa-sha2-256 | rsa-sha2-512 | ssh-rsa }
```

Mode

Cipher Control SSH

Description

Disable ssh public key algorithm.

Options

rsa-sha2-256 Rsa-sha2-256.

rsa-sha2-512 Rsa-sha2-512.

ssh-rsa Ssh-rsa.

Example

```
no public-key ssh-rsa
```

Syntax

```
public-key { rsa-sha2-256 | rsa-sha2-512 | ssh-rsa }
```

Mode

Cipher Control SSH

Description

Enable ssh public key algorithm.

Options

rsa-sha2-256 Rsa-sha2-256.

rsa-sha2-512 Rsa-sha2-512.

ssh-rsa Ssh-rsa.

Example

```
public-key ssh-rsa
```

Syntax

```
no encryption { aes128-ctr | aes128-gcm | aes192-ctr | aes256-ctr | aes256-gcm | chacha20-poly1305 }
```

Mode

Cipher Control SSH

Description

Disable ssh encryption algorithm.

Options

aes128-ctr Aes128-ctr.

aes128-gcm Aes128-gcm@openssh.com.

aes192-ctr Aes192-ctr.

<i>aes256-ctr</i>	Aes256-ctr.
<i>aes256-gcm</i>	Aes256-gcm@openssh.com.
<i>chacha20-poly1305</i>	Chacha20-poly1305@openssh.com.

Example

```
no encryption aes192-ctr
```

Syntax

```
encryption { aes128-ctr | aes128-gcm | aes192-ctr | aes256-ctr | aes256-gcm | chacha20-poly1305 }
```

Mode

Cipher Control SSH

Description

Enable ssh encryption algorithm.

Options

<i>aes128-ctr</i>	Aes128-ctr.
<i>aes128-gcm</i>	Aes128-gcm@openssh.com.
<i>aes192-ctr</i>	Aes192-ctr.
<i>aes256-ctr</i>	Aes256-ctr.
<i>aes256-gcm</i>	Aes256-gcm@openssh.com.
<i>chacha20-poly1305</i>	Chacha20-poly1305@openssh.com.

Example

```
encryption aes192-ctr
```

Syntax

```
no mac { hmac-sha1 | hmac-sha2-256 | hmac-sha2-512 }
```

Mode

Cipher Control SSH

Description

Disable ssh MAC algorithm.

Options

<i>hmac-sha1</i>	Hmac-sha1.
<i>hmac-sha2-256</i>	Hmac-sha2-256.
<i>hmac-sha2-512</i>	Hmac-sha2-512.

Example

```
no mac hmac-sha1
```

Syntax

```
mac { hmac-sha1 | hmac-sha2-256 | hmac-sha2-512 }
```

Mode

Cipher Control SSH

Description

Enable ssh MAC algorithm.

Options

hmac-sha1 Hmac-sha1.

hmac-sha2-256 Hmac-sha2-256.

hmac-sha2-512 Hmac-sha2-512.

Example

```
mac hmac-sha1
```

Syntax

```
udp [ ipv6 ]
```

Mode

Config

Description

Configure UDP settings.

Options

ipv6 Configure UDPv6 settings.

Example

```
udp
udp ipv6
```

Syntax

```
default-connection-timeout <UINT32>
```

Mode

UDP
UDPv6

Description

Set default UDP connection timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
default-connection-timeout 15
```

Syntax

flood protection

Mode

UDP
UDIPv6

Description

Enable UDP flood protection.

Example

flood protection

Syntax

no flood protection

Mode

UDP
UDIPv6

Description

Disable UDP flood protection.

Example

no flood protection

Syntax

flood attack-threshold <UINT32>

Mode

UDP
UDIPv6

Description

Set UDP flood attack threshold (UDP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

flood attack-threshold 1000

Syntax

flood block-timeout <UINT8>

Mode

UDP
UDIPv6

Description

Set UDP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

flood block-timeout 2

Syntax

flood protected-dest-list { any | fqdn <ADDR_FQDN> | group <ADDR_FHNRM_GROUP_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <UDP_FLOOD_PROTECTED_DESTINATION_LIST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

UDP
UDIPv6

Description

Set UDP flood attack protected destination list.

Options

any	Set UDP flood attack protected destination list to any.
fqdn <ADDR_FQDN>	FQDN. FQDN in the form: example.com or *.example.com. Example: example.com
group <ADDR_FHNRM_GROUP_WITH_MIXED>	Set UDP flood attack protected destination list to named address group. FQDN/host/network/range/mac group address object name. Example: Web Server Group
host <ADDR_HOST>	Set UDP flood attack protected destination list as host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n
mac <ADDR_MAC>	Set UDP flood attack protected destination list as mac address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <UDP_FLOOD_PROTECTED_DESTINATION_LIST_NAME>	Set UDP flood attack protected destination list to named address object. FQDN/host/network/range/mac address object name. Example: Web Server
network <ADDR_NETWORK> <ADDR_MASK>	Set UDP flood attack protected destination list to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: IPV4: 255.255.255.0\nIPV6: /64\n
range <ADDR_BEGIN> <ADDR_END>	Set UDP flood attack protected destination list to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n

Example

flood protected-dest-list any

Syntax

clear udp statistics

Mode

UDP
UDIPv6

Description

Clear UDP traffic statistics.

Example

```
clear udp statistics
```

Syntax

```
icmp [ ipv6 ]
```

Mode

Config

Description

Configure ICMP settings.

Options

ipv6 Configure ICMPv6 settings.

Example

```
icmp  
icmp ipv6
```

Syntax

```
flood protection
```

Mode

ICMP
ICMPv6

Description

Enable ICMP flood protection.

Example

```
flood protection
```

Syntax

```
no flood protection
```

Mode

ICMP
ICMPv6

Description

Disable ICMP flood protection.

Example

```
no flood protection
```

Syntax

flood attack-threshold <UINT32>

Mode

ICMP
ICMPv6

Description

Set ICMP flood attack threshold (ICMP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

flood attack-threshold 1000

Syntax

flood block-timeout <UINT8>

Mode

ICMP
ICMPv6

Description

Set ICMP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

flood block-timeout 2

Syntax

flood protected-dest-list { any | fqdn <ADDR_FQDN> | group <ADDR_FHNR_GROUP_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ICMP_FLOOD_PROTECTED_DESTINATION_LIST_NAME> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

ICMP
ICMPv6

Description

Set ICMP flood attack protected destination list.

Options

any Set ICMP flood attack protected destination list to any.

fqdn FQDN.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Set ICMP flood attack protected destination list to named address group.
<ADDR_FHNR_GROUP_WITH_MIXED> FQDN/host/network/range group address object name.
Example: *Web Server Group*

host Set ICMP flood attack protected destination list as host address.

<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Set ICMP flood attack protected destination list as mac address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ICMP_FLOOD_PROTECTED_DESTINATION_LIST_NAME>	Set ICMP flood attack protected destination list to named address object. FQDN/host/network/range/mac address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Set ICMP flood attack protected destination list to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range <ADDR_BEGIN>	Set ICMP flood attack protected destination list to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
flood-protected-dest-list any
```

Syntax

```
clear icmp statistics
```

Mode

ICMP
ICMPv6

Description

Clear ICMP traffic statistics.

Example

```
clear icmp statistics
```

Syntax

```
dynamic-external-object <DYNAMIC_EXTERNAL_OBJECT_NAME>
```

Mode

Config

Description

Add/edit dynamic external object.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME> Dynamic external object name.
Example: *abc*

Example

```
dynamic-external-object "Dynamic Guests"
```

Syntax

no dynamic-external-object <DYNAMIC_EXTERNAL_OBJECT_NAME>

Mode

Config

Description

Delete dynamic external object.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME> Dynamic external object name.
Example: *abc*

Example

no dynamic-external-object "Dynamic Guests"

Syntax

no dynamic-external-objects

Mode

Config

Description

Delete all dynamic external objects.

Example

no dynamic-external-objects

Syntax

type address-group

Mode

Dynamic External Object

Description

Set the dynamic external object type.

Example

type address-group

Syntax

name <DYNAMIC_EXTERNAL_OBJECT_NAME>

Mode

Dynamic External Object

Description

Edit dynamic external object name.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME> Dynamic external object name.
Example: *abc*

Example

```
name "Dynamic Guests"
```

Syntax

```
zone <ZONE_NAME>
```

Mode

Dynamic External Object

Description

Set dynamic external object zone.

Options

<ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
zone WAN
```

Syntax

```
fqdn
```

Mode

Dynamic External Object

Description

Enable dynamic external object FQDN flag.

Example

```
fqdn
```

Syntax

```
no fqdn
```

Mode

Dynamic External Object

Description

Disable dynamic external object FQDN flag.

Example

```
no fqdn
```

Syntax

```
periodic-download [ interval { 1-hour | 15-minutes | 24-hours | 5-minutes } ]
```

Mode

Dynamic External Object

Description

Enable dynamic external object periodic download.

Options

<i>interval</i>	Set the dynamic external object periodic download interval.
<i>1-hour</i>	1 hour.
<i>15-minutes</i>	15 minutes.
<i>24-hours</i>	24 hours.
<i>5-minutes</i>	5 minutes.

Example

```
periodic-download interval 600
```

Syntax

```
no periodic-download
```

Mode

Dynamic External Object

Description

Disable dynamic external object periodic download.

Example

```
no periodic-download
```

Syntax

```
protocol { ftp | https }
```

Mode

Dynamic External Object

Description

Set the dynamic external object download protocol.

Options

<i>ftp</i>	FTP.
<i>https</i>	HTTPS.

Example

```
protocol https
```

Syntax

```
url <URL>
```

Mode

Dynamic External Object

Description

Set the external dynamic object HTTPS URL.

Options

<URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
url "10.10.10.10/uploads/dynamicObjects/dynamicGuest.txt"
```

Syntax

```
no url
```

Mode

Dynamic External Object

Description

Clear the external dynamic object HTTPS URL.

Example

```
no url
```

Syntax

```
server <IPV4_HOST>
```

Mode

Dynamic External Object

Description

Set the external dynamic object FTP server's IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
server 192.168.168.75
```

Syntax

```
no server
```

Mode

Dynamic External Object

Description

Clear the external dynamic object FTP server's IP address.

Example

```
no server
```

Syntax


```
login <WORD>
```

Mode

Dynamic External Object

Description

Set the external dynamic object FTP server's login name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
login admin@testing.local
```

Syntax

```
no login
```

Mode

Dynamic External Object

Description

Clear the external dynamic object FTP server's login name.

Example

```
no login
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

Dynamic External Object

Description

Set the external dynamic object FTP server's login password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password myftppassword
```

Syntax

```
no password
```

Mode

Dynamic External Object

Description

Clear the external dynamic object FTP server's login password.

Example

no password

Syntax

directory <WORD>

Mode

Dynamic External Object

Description

Set the external dynamic object FTP server's directory path.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

directory uploads/dynamicObjects/

Syntax

no directory

Mode

Dynamic External Object

Description

Clear the external dynamic object FTP server's directory path.

Example

no directory

Syntax

filename <WORD>

Mode

Dynamic External Object

Description

Set the external dynamic object FTP server's filename.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

filename dynamicGuest.txt

Syntax

no filename

Mode

Description

Clear the external dynamic object FTP server's filename.

Example

```
no filename
```

Syntax

```
clear dynamic-external-object statistics <DYNAMIC_EXTERNAL_OBJECT_NAME>
```

Mode

Config

Description

Clear the dynamic external object statistics.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME> Dynamic external object name.
Example: *abc*

Example

```
clear dynamic-external-object statistics test
```

Syntax

```
download dynamic-external-object <DYNAMIC_EXTERNAL_OBJECT_NAME>
```

Mode

Config

Description

Download the dynamic external object file now.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME> Dynamic external object name.
Example: *abc*

Example

```
download dynamic-external-object test
```

Syntax

```
qos-mapping cos <UINT8> [ to-dscp <UINT8> ] [ from-dscp <UINT8> <UINT8> ]
```

Mode

Config

Description

Configure QoS mapping.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

to-dscp Set the DSCP value to map to.

- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*
- from-dscp** Set the from DSCP range.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*

Example

```
qos-mapping cos 0 to-dscp 1 from-dscp 1 6
```

Syntax

```
qos-mapping reset
```

Mode

Config

Description

Reset QoS mapping settings.

Example

```
qos-mapping reset
```

Syntax

```
show firewall [ connection-status ]
```

Mode

All Modes

Description

Show firewall settings.

Options

- connection-status** Show firewall connections status.

Example

```
show firewall
```

Syntax

```
show multicast [ { pending-config | with-pending-config } | state { entries | entry address <MULTICAST_GROUP_IPV4_HOST> interface <MULTICAST_INTERFACE> } ]
```

Mode

All Modes

Description

Show multicast configuration.

Options

- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

state	Show multicast state.
entries	Show multicast state entries.
entry	Show a specified multicast state entry.
address	Multicast group address.
<MULTICAST_GROUP_IPV4_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
interface	Interface or vpn tunnel.
<MULTICAST_INTERFACE>	Multicast interface name. Example: <i>X0</i>

Example

```
show multicast
show multicast state entries
show multicast state entry address 192.168.168.10 interface X0
```

Syntax

```
show access-rule ipv4 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source {
[ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group
<SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] ] [ service { { any |
group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [
address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] ] [ schedule { { always-on
| days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ statistics ] [ connection-limit top
<UINT8> ] [ { pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show an access rule.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Destination service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>

host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
statistics	Show statistics for specified access rule.
connection-limit	Show connection statistics of the access rule which has enabled source or destination IP address connection limit.
top	Show access rule top connection statistics.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show access-rule ipv4 from LAN to WLAN action allow
```

Syntax

```
show access-rule ipv4 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv4 access rule for associated UUID.

Options

<UUID> Universally Unique Identifier (UUID).

Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show access-rule ipv4 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show access-rules [ [ [ ipv4 | ipv6 ] [ connection-limit | from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> | unused ] [ statistics ] [ { custom | default } ] [ { pending-config | with-pending-config } ] ] | max-count ]
```

Mode

All Modes

Description

Show all access rules.

Options

<i>ipv4</i>	Show IPv4 access rules.
<i>ipv6</i>	Show IPv6 access rules.
<i>connection-limit</i>	Show access rules that enabled and on which source or destination IP address connection limit is enabled.
<i>from</i>	Source zone.
<i><ACCESS_RULE_ZONE_NAME></i>	Access rule from. Example: <i>DMZ</i>
<i>to</i>	Destination zone.
<i><ACCESS_RULE_ZONE_NAME></i>	Access rule from. Example: <i>DMZ</i>
<i>unused</i>	Show access rules assigned to a Zone that has not been assigned to an interface.
<i>statistics</i>	Show statistics for all access rules.
<i>custom</i>	Show custom configuration.
<i>default</i>	Show system/factory default configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>max-count</i>	Show access rules max count.

Example

```
show access-rules
show access-rules from * to WAN
show access-rules from DMZ to WAN
```

Syntax

```
show access-rule ipv6 from <ACCESS_RULE_ZONE_NAME> to <ACCESS_RULE_ZONE_NAME> action { { allow | deny | discard } } [ source { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] } ] [ service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } } ] [ destination { [ address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name
```



```
<ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } ] [ schedule { { always-on
| days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } } ] [ connection-limit top <UINT8> ] [ {
pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an access rule.

Options

<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
to	Destination Zone.
<ACCESS_RULE_ZONE_NAME>	Access rule from. Example: <i>DMZ</i>
action	Set the action for this access rule.
allow	Allow traffic matching the criteria.
deny	Deny traffic matching the criteria.
discard	Discard traffic matching the criteria.
source	Source.
address	Source address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
port	Source port.
any	Any source service.
group	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>

name	Source service Object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Source service Object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
service	Destination service.
any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
destination	Destination.
address	Destination address.
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
schedule	Schedule.
always-on	Always on.

days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
connection-limit	Show connection statistics of the access rule which has enabled source or destination IP address connection limit.
top	Show access rule top connection statistics.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show access-rule ipv6 from LAN to WLAN action allow
```

Syntax

```
show access-rule ipv6 uuid <UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an IPv6 access rule for associated UUID.

Options

<UUID>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show access-rule ipv6 uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
show ssl-control [ base | blacklist-certificate <BLACKLIST_CERTIFICATE> | blacklist-certificates | whitelist-certificate <WHITELIST_CERTIFICATE> | whitelist-certificates ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSL control configuration.

Options

base	Show SSL control base settings.

<i>blacklist-certificate</i>	Show one specific SSL control blacklist certificate.
<i><BLACKLIST_CERTIFICATE></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>certificateName</i>
<i>blacklist-certificates</i>	Show SSL control blacklist certificates configuration.
<i>whitelist-certificate</i>	Show one SSL control whitelist certificate.
<i><WHITELIST_CERTIFICATE></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>certificateName</i>
<i>whitelist-certificates</i>	Show SSL control whitelist certificates configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show ssl-control
```



Syntax

```
show tcp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show TCP configuration or traffic statistics.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show TCP statistics.

Example

```
show tcp
```



Syntax

```
show bandwidth-objects [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all bandwidth objects.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

Syntax

```
show bandwidth-object <BANDWIDTH_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a bandwidth object.

Options

<BANDWIDTH_OBJ_NAME>	Bandwidth object name. Example: <code>\ "Corp High Priority" \</code>
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show bandwidth-object "Corp High Priority"
```

Syntax

```
show cipher-control tls-cipher-list [ strength { all | insecure | recommended | secure | weak } action { all | allow | block }  
cbc { all | is | not } [ tls10 ] [ tls11 ] [ tls12 ] [ tls13 ] ]
```

Mode

All Modes

Description

Show cipher control tls list by filter and if applicable to DPI-SSL, HTTPS management, and control.

Options

<i>strength</i>	Cipher strength.
<i>all</i>	Ciphers of all strengths.
<i>insecure</i>	Ciphers of insecure strength.
<i>recommended</i>	Ciphers of recommended strength.
<i>secure</i>	Ciphers of secure strength.
<i>weak</i>	Ciphers of weak strength.
<i>action</i>	Cipher current action.
<i>all</i>	Ciphers that are currently set to blocked or unblocked.
<i>allow</i>	Ciphers that are currently set to unblocked.
<i>block</i>	Ciphers that are currently set to blocked.
<i>cbc</i>	Cipher CBC status.
<i>all</i>	Ciphers that do and don't use block chaining.
<i>is</i>	Ciphers that use block chaining.
<i>not</i>	Ciphers that don't use block chaining.
<i>tls10</i>	Include TLS1.0 Ciphers.

<i>tls11</i>	Include TLS1.1 Ciphers.
<i>tls12</i>	Include TLS1.2 Ciphers.
<i>tls13</i>	Include TLS1.3 Ciphers.

Example

```
show cipher-control tls-cipher-list
```

Syntax

```
show cipher-control ssh [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSH cipher control configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show cipher-control ssh
```

Syntax

```
show udp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show UDP configuration or traffic statistics.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.
- statistics*** Show UDP statistics.

Example

```
show udp
```

Syntax

```
show udpv6 [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show UDPv6 configuration or traffic statistics.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show UDP statistics.

Example

```
show udpv6
```

Syntax

```
show icmp [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show ICMP configuration or traffic statistics.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show ICMP statistics.

Example

```
show icmp
```

Syntax

```
show icmpv6 [ { pending-config | with-pending-config } | statistics ]
```

Mode

All Modes

Description

Show ICMPv6 configuration or traffic statistics.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show ICMP statistics.

Example

```
show icmpv6
```

Syntax

```
show dynamic-external-object <DYNAMIC_EXTERNAL_OBJECT_NAME> [ group-members ] [ statistics ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show dynamic external object.

Options

<DYNAMIC_EXTERNAL_OBJECT_NAME>	Dynamic external object name. Example: <i>abc</i>
group-members	Group members.
statistics	Statistics.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show dynamic-external-object
```

Syntax

```
show dynamic-external-objects [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all dynamic external objects.

Options

pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show dynamic-external-objects
```

Syntax

```
show qos-mapping [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show QoS mapping.

Options

pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show qos-mapping

Syntax

administration

Mode

Config

Description

Administration settings.

Example

administration

Syntax

firewall-name <WORD>

Mode

Administration

Description

Set the name for the firewall.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

firewall-name "ACME Corporate Firewall"

Syntax

no firewall-name

Mode

Administration

Description

Clear the name for the firewall.

Example

no firewall-name

Syntax

auto-append-suffix

Mode

Administration

Description

Enable auto-append suffix to firewall name.

Example

```
auto-append-suffix
```

Syntax

```
no auto-append-suffix
```

Mode

Administration

Description

Disable auto-append suffix to firewall name.

Example

```
no auto-append-suffix
```

Syntax

```
cloud-backup-enable
```

Mode

Administration

Description

Enable cloud backup.

Example

```
cloud-backup-enable
```

Syntax

```
no cloud-backup-enable
```

Mode

Administration

Description

Disable cloud-backup.

Example

```
no cloud-backup-enable
```

Syntax

```
firewall-domain-name <WORD>
```

Mode

Administration

Description

Set the domain name for the firewall.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

firewall-domain-name "ACME Corporate"

Syntax

no firewall-domain-name

Mode

Administration

Description

Clear the domain name for the firewall.

Example

no firewall-domain-name

Syntax

language-override { chinese | chinese-traditional | english | japanese | korean | portuguese }

Mode

Administration

Options

<i>chinese</i>	Chinese.
<i>chinese-traditional</i>	Chinese (Traditional).
<i>english</i>	English.
<i>japanese</i>	Japanese.
<i>korean</i>	Korean.
<i>portuguese</i>	Portuguese.

Example

language-override english

Syntax

no language-override

Mode

Administration

Example

no language-override

Syntax

admin name <WORD>

Mode

Administration

Description

Set the name for the built in administrator.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

admin name headhoncho

Syntax

admin password old-password <WORD> new-password <WORD> confirm-password <WORD>

Mode

Administration

Description

Set the password for the built in administrator.

Options

old-password Enter the old password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
new-password Enter the new password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
confirm-password Confirm the new password.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

admin password old-password passwd new-password smorgasbord confirm-password smorgasbord

Syntax

admin one-time-password totp

Mode

Administration

Description

Set admin one-time passwords method.

Example

admin one-time-password totp

Syntax

no admin one-time-password

Mode

Administration

Description

Disable one-time password required for the admin.

Example

```
no admin one-time-password
```

Syntax

```
admin unbind-totp-key
```

Mode

Administration

Description

Unbind admin totp key.

Example

```
admin unbind-totp-key
```

Syntax

```
wireless-lan
```

Mode

Administration

Description

Enable wireless LAN.

Example

```
wireless-lan
```

Syntax

```
no wireless-lan
```

Mode

Administration

Description

Disable wireless LAN.

Example

```
no wireless-lan
```

Syntax

```
ipv6
```

Mode

Administration

Description

Enable IPv6.

Example

```
ipv6
```

Syntax

```
no ipv6
```

Mode

Administration

Description

Disable IPv6.

Example

```
no ipv6
```

Syntax

```
password aging duration <UINT16>
```

Mode

Administration

Description

Enable that password must be changed every set number of days and configure duration.

Options

- duration** Set the number of days before the password must be changed.
- <UINT16>** Integer in the form: D OR 0xHHHHH.
Example: *123*

Example

```
password aging duration 90
```

Syntax

```
no password aging
```

Mode

Administration

Description

Disable that password must be changed every set number of days.

Example

```
no password aging
```

Syntax

```
password last-changed period <UINT16>
```

Mode

Administration

Description

Enable that password must not be changed before the set number of days and configure duration.

Options

period Set the number of days before the password must not be changed.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
password last-changed period 2
```

Syntax

```
no password last-changed
```

Mode

Administration

Description

Disable that password must not be changed every set number of days.

Example

```
no password last-changed
```

Syntax

```
password uniqueness count <UINT8>
```

Mode

Administration

Description

Enable barring of repeated passwords and configure.

Options

count Set the number of password changes before repeated password are allowed.
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
password uniqueness count 5
```

Syntax

```
no password uniqueness
```

Mode

Administration

Description

Disable barring of repeated passwords.

Example

```
no password uniqueness
```

Syntax

password enforce-character-difference

Mode

Administration

Description

Enable new password must contain 4 characters different from the old password.

Example

password enforce-character-difference

Syntax

no password enforce-character-difference

Mode

Administration

Description

Disable new password must contain 4 characters different from the old password.

Example

no password enforce-character-difference

Syntax

password minimum-length <UINT8>

Mode

Administration

Description

Set the minimum password length to enforce.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

password minimum-length 8

Syntax

password complexity alpha-and-numeric-and-symbols

Mode

Administration

Description

Set the allowed complexity of the password.

Example

password complexity alpha-and-numeric-and-symbols

Syntax

password complexity alpha-and-numeric

Mode

Administration

Description

Set the allowed complexity of the password.

Example

password complexity alpha-and-numeric

Syntax

no password complexity [digital | lower-case | symbolic | upper-case]

Mode

Administration

Description

Clear password complexity.

Options

- digital*** Set minimum digital character number.
- lower-case*** Set minimum lower case character number.
- symbolic*** Set minimum symbolic character number.
- upper-case*** Set minimum upper case character number.

Example

no password complexity

Syntax

password complexity type { alpha-and-numeric | alpha-and-numeric-and-symbols }

Mode

Administration

Description

Set the allowed complexity of the password.

Options

- alpha-and-numeric*** Must contain both numbers and letters.
- alpha-and-numeric-and-symbols*** Must contain numbers, letters, and symbols.

Example

password complexity alpha-and-numeric-and-symbols

Syntax

password complexity upper-case <UINT16>

Mode

Administration

Description

Set the upper-case complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

password complexity upper-case 1

Syntax

password complexity lower-case <UINT16>

Mode

Administration

Description

Set the lower-case complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

password complexity lower-case 1

Syntax

password complexity digital <UINT16>

Mode

Administration

Description

Set the digital complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

password complexity digital 1

Syntax

password complexity symbolic <UINT16>

Mode

Administration

Description

Set the symbolic complexity of the password.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

password complexity symbolic 1

Syntax

password constraints-apply-to [builtin-admin] [full-admins] [limited-admins] [local-users] [guest-admins] [system-admins] [crypto-admins] [audit-admins]

Mode

Administration

Description

Set whom to apply the password constraints to.

Options

builtin-admin	Built in administrator.
full-admins	Other full administrators.
limited-admins	Limited administrators.
local-users	Other local users.
guest-admins	Guest admins.
system-admins	System administrators
crypto-admins	Crypto administrators
audit-admins	Audit administrators

Example

password constraints-apply-to builtin-admin full-admins

Syntax

no password constraints-apply-to [builtin-admin] [full-admins] [limited-admins] [local-users] [guest-admins] [system-admins] [crypto-admins] [audit-admins]

Mode

Administration

Description

Remove setting of whom to apply the password constraints to.

Options

builtin-admin	Built in administrator.
full-admins	Other full administrators.
limited-admins	Limited administrators.
local-users	Other local users.
guest-admins	Guest admins.
system-admins	System administrators
crypto-admins	Crypto administrators
audit-admins	Audit administrators

Example

no password constraints-apply-to builtin-admin full-admins

Syntax

idle-logout-time <UINT16>

Mode

Administration

Description

Set the allowed period of inactivity before administrators are logged out of the management interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

idle-logout-time 60

Syntax

user-lockout { enable | failures-duration <UINT8> | failures-rate <UINT8> | lockout-duration <UINT8> }

Mode

Administration

Description

Enable administrator / user lockout and set conditions.

Options

enable	Enable administrator / user lockout configure.
failures-duration <UINT8>	Set the failed in designed duration before lockout. Integer in the form: D OR 0xHH. Example: <i>123</i>
failures-rate <UINT8>	Set the failed login attempts in designed duration before lockout. Integer in the form: D OR 0xHH. Example: <i>123</i>
lockout-duration <UINT8>	Set number of minutes a user should be locked out. Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

user-lockout enable
user-lockout failures-rate 5
user-lockout failures-duration 5
user-lockout lockout-duration 10

Syntax

no user-lockout enable

Mode

Administration

Description

Disable administrator / user lockout for set conditions.

Options

enable Enable administrator / user lockout configure.

Example

```
no user-lockout enable
```

Syntax

```
local-user-lockout
```

Mode

Administration

Description

Enable local administrator/user account lockout (uncheck for login IP address lockout).

Example

```
local-user-lockout
```

Syntax

```
no local-user-lockout
```

Mode

Administration

Description

Disable local administrator/user account lockout (uncheck for login IP address lockout).

Example

```
no local-user-lockout
```

Syntax

```
log-without-lockout
```

Mode

Administration

Description

Enable Log event only without lockout.

Example

```
log-without-lockout
```

Syntax

```
no log-without-lockout
```

Mode

Administration

Description

Disable Log event only without logout.

Example

```
no log-without-logout
```

Syntax

```
max-login-attempts-cli <UINT8>
```

Mode

Administration

Description

Configure max login attempts through CLI.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
max-login-attempts-cli 2
```

Syntax

```
admin preempt-action { goto-non-config | logout }
```

Mode

Administration

Description

Set action to do upon preemption by another administrator.

Options

goto-non-config Drop to non-config mode.

logout Logout.

Example

```
admin preempt-action logout
```

Syntax

```
admin preempt-inactivity-timeout <UINT16>
```

Mode

Administration

Description

Allow preemption by a lower priority administrator after inactivity of (minutes).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
admin preempt-inactivity-timeout 10
```

Syntax

```
inter-admin-messaging <UINT8>
```

Mode

Administration

Description

Enable inter administrator messaging and set the messaging polling interval.

Options

<*UINT8*> Integer in the form: D OR 0xHH.
Example: 123

Example

```
inter-admin-messaging 10
```

Syntax

```
no inter-admin-messaging
```

Mode

Administration

Description

Disable inter-administrator messaging.

Example

```
no inter-admin-messaging
```

Syntax

```
multiple-admin
```

Mode

Administration

Description

Enable multiple administrative roles.

Example

```
multiple-admin
```

Syntax

```
no multiple-admin
```

Mode

Administration

Description

Disable multiple administrative roles.

Example

```
no multiple-admin
```

Syntax

```
enhanced-audit-logging
```

Mode

Administration

Description

Enable enhanced audit logging.

Example

```
enhanced-audit-logging
```

Syntax

```
no enhanced-audit-logging
```

Mode

Administration

Description

Disable enhanced audit logging.

Example

```
no enhanced-audit-logging
```

Syntax

```
wireless-controller-mode { non-wireless-controller | normal-firewall | wireless-controller }
```

Mode

Administration

Description

Set wireless controller mode.

Options

non-wireless-controller Set wireless controller as non wireless controller mode.

normal-firewall Set wireless controller as normal firewall mode.

wireless-controller Set wireless controller as wireless controller mode.

Example

```
wireless-controller-mode normal-firewall
```

Syntax


```
web-management allow-http
```

Mode

Administration

Description

Allow HTTP management (it is less secure than using HTTPS).

Example

```
web-management allow-http
```

Syntax

```
no web-management allow-http
```

Mode

Administration

Description

Do not allow HTTP management (it is less secure than using HTTPS).

Example

```
no web-management allow-http
```

Syntax

```
http-port <IPV4_PORT>
```

Mode

Administration

Description

Set the HTTP management port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
http-port 8080
```

Syntax

```
https-port <IPV4_PORT>
```

Mode

Administration

Description

Set the HTTPS management port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

Syntax

web-management certificate { name <CERT_NAME> | use-self-signed }

Mode

Administration

Description

Set the HTTPS management server certificate to use.

Options

- name** Specify certificate.
- <CERT_NAME>** Certificate name.
Example: *my_cert*
- use-self-signed** Use self signed certificate.

Example

web-management certificate name "ACME Inc."

Syntax

web-management cert-common-name <WORD>

Mode

Administration

Description

Set the self signed certificate common name.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

web-management cert-common-name www.acme.com

Syntax

no web-management cert-common-name

Mode

Administration

Description

Clear the self signed certificate common name.

Example

no web-management cert-common-name

Syntax

web-management client-certificate-check

Mode

Administration

Description

Enable client certificate check.

Example

web-management client-certificate-check

Syntax

no web-management client-certificate-check

Mode

Administration

Description

Disable client certificate check.

Example

no web-management client-certificate-check

Syntax

web-management client-certificate-cache

Mode

Administration

Description

Enable client certificate cache.

Example

web-management client-certificate-cache

Syntax

no web-management client-certificate-cache

Mode

Administration

Description

Disable client certificate cache.

Example

no web-management client-certificate-cache

Syntax

web-management user-name-field { common-name | email | principal-name }

Mode

Administration

Description

Set user name field.

Options

- common-name*** Set user-name-field common-name.
- email*** Set user-name-field email.
- principal-name*** Set user-name-field principal-name.

Example

```
web-management user name field common-name
```

Syntax

```
web-management client-certificate-issuer <CERT_ISSUER>
```

Mode

Administration

Description

Set client certificate issuer.

Options

- <CERT_ISSUER>*** Certificate Issuer.
Example: *Thawte Server CA*

Example

```
web-management client-certificate-issuer "Thawte Premium Server CA"
```

Syntax

```
web-management cac-user-group-retrieve { from-ldap | local-configured }
```

Mode

Administration

Description

Set user name field.

Options

- from-ldap*** Set cac-user-group-retrieve from-ldap.
- local-configured*** Set cac-user-group-retrieve local-configured.

Example

```
web-management cac user group retrieve local-configured
```

Syntax

```
web-management ocsp-check <URL>
```

Mode

Administration

Description

Enable ocap check.

Options

<URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
web-management ocap-check http://www.example.com/products/
```

Syntax

```
no web-management ocap-check
```

Mode

Administration

Description

Disable ocap check.

Example

```
no web-management ocap-check
```

Syntax

```
web-management ocap-periodic-check enable
```

Mode

Administration

Description

Disable tooltips in web management UI and configure.

Example

```
no web-management tooltip
```

Syntax

```
no web-management ocap-periodic-check enable
```

Mode

Administration

Description

Disable tooltips in web management UI and configure.

Example

```
no web-management tooltip
```

Syntax

```
web-management oosp_check_interval <UINT32>
```

Mode

Administration

Description

Set web-management oosp_check_interval (in hours).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
web-management oosp_check_interval 24
```

Syntax

```
web-management default-table-size <UINT16>
```

Mode

Administration

Description

Set default size of tables within the Web Management User Interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
web-management default-table-size 50
```

Syntax

```
web-management refresh-interval <UINT16>
```

Mode

Administration

Description

Set auto-update refresh interval of tables within the web management user interface.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
web-management refresh-interval 15
```

Syntax

```
web-management tooltip { button-delay <UINT16> | enable | form-delay <UINT16> | text-delay <UINT16> }
```

Mode

Administration

Description

Enable tooltips in web management UI and configure.

Options

- button-delay***

Set button tooltip delay.
- <UINT16>***

Integer in the form: D OR 0xHHHH.
Example: *123*
- enable***

Enable tooltips in web management configure.
- form-delay***

Set form tooltip delay.
- <UINT16>***

Integer in the form: D OR 0xHHHH.
Example: *123*
- text-delay***

Set text tooltip delay.
- <UINT16>***

Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
web-management tooltip enable
web-management tooltip form-delay 2000
web-management tooltip button-delay 3000
web-management tooltip text-delay 500
```

Syntax

```
no web-management tooltip enable
```

Mode

Administration

Description

Disable tooltips in web management UI and configure.

Options

- enable***

Enable tooltips in web management configure.

Example

```
no web-management tooltip
```

Syntax

```
web-management certification-periodic-expiration-check
```

Mode

Administration

Description

Enable certification periodic expiration check.

Example

```
web-management certification-periodic-expiration-check
```

Syntax

```
no web-management certification-periodic-expiration-check
```

Mode

Administration

Description

Disabled certification Periodic Expiration check.

Example

```
no web-management certification-periodic-expiration-check
```

Syntax

```
web-management certification-expiration-interval <UINT16>
```

Mode

Administration

Description

Set default certication expiration interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
web-management certification-expiration-interval 168
```

Syntax

```
uuid all
```

Mode

Administration

Description

Enable show UUIDs for all.

Example

```
uuid all
```

Syntax

```
no uuid all
```

Mode

Administration

Description

Disable show UUIDs for all.

Example

```
no uuid all
```

Syntax

uuid address-objects

Mode

Administration

Description

Enable show UUID for address-objects.

Example

uuid address-objects

Syntax

no uuid address-objects

Mode

Administration

Description

Disable show UUID for address-objects.

Example

no uuid address-objects

Syntax

uuid service-objects

Mode

Administration

Description

Enable show UUID for service-objects.

Example

uuid service-objects

Syntax

no uuid service-objects

Mode

Administration

Description

Disable show UUID for service-objects.

Example

no uuid service-objects

Syntax

uuid user-objects

Mode

Administration

Description

Enable show UUID for user-objects.

Example

```
uuid user-objects
```

Syntax

```
no uuid user-objects
```

Mode

Administration

Description

Disable show UUID for user-objects.

Example

```
no uuid user-objects
```

Syntax

```
uuid schedule-objects
```

Mode

Administration

Description

Enable show UUID for schedule-objects.

Example

```
uuid schedule-objects
```

Syntax

```
no uuid schedule-objects
```

Mode

Administration

Description

Disable show UUID for schedule-objects.

Example

```
no uuid schedule-objects
```

Syntax

```
uuid zone-objects
```

Mode

Administration

Description

Enable show UUID for zone-objects.

Example

```
uuid zone-objects
```

Syntax

```
no uuid zone-objects
```

Mode

Administration

Description

Disable show UUID for zone-objects.

Example

```
no uuid zone-objects
```

Syntax

```
uuid access-rules
```

Mode

Administration

Description

Enable show UUID for access-rules.

Example

```
uuid access-rules
```

Syntax

```
no uuid access-rules
```

Mode

Administration

Description

Disable show UUID for access-rules.

Example

```
no uuid access-rules
```

Syntax

```
uuid nat-policy
```

Mode

Administration

Description

Enable show UUID for nat-policy.

Example

uuid nat-policy

Syntax

no uuid nat-policy

Mode

Administration

Description

Disable show UUID for nat-policy.

Example

no uuid nat-policy

Syntax

uuid routing-policy

Mode

Administration

Description

Enable show UUID for routing-policy.

Example

uuid routing-policy

Syntax

no uuid routing-policy

Mode

Administration

Description

Disable show UUID for routing-policy.

Example

no uuid routing-policy

Syntax

uuid content-filter-objects

Mode

Administration

Description

Enable show UUID for content-filter-objects.

Example

uuid content-filter-objects

Syntax

```
no uuid content-filter-objects
```

Mode

Administration

Description

Disable show UUID for content-filter-objects.

Example

```
no uuid content-filter-objects
```

Syntax

```
uuid content-filter-policies
```

Mode

Administration

Description

Enable show UUID for content-filter-policies.

Example

```
uuid content-filter-policies
```

Syntax

```
no uuid content-filter-policies
```

Mode

Administration

Description

Disable show UUID for content-filter-policies.

Example

```
no uuid content-filter-policies
```

Syntax

```
uuid network-monitor-policy
```

Mode

Administration

Description

Enable show UUID for network-monitor-policy.

Example

```
uuid network-monitor-policy
```

Syntax

```
no uuid network-monitor-policy
```

Mode

Administration

Description

Disable show UUID for network-monitor-policy.

Example

```
no uuid network-monitor-policy
```

Syntax

```
uuid sdwan-performance-probes
```

Mode

Administration

Description

Enable show UUID for sdwan-performance-probes.

Example

```
uuid sdwan-performance-probes
```

Syntax

```
no uuid sdwan-performance-probes
```

Mode

Administration

Description

Disable show UUID for sdwan-performance-probes.

Example

```
no uuid sdwan-performance-probes
```

Syntax

```
dashboard-as-starting-page
```

Mode

Administration

Description

Use dashboard as starting page.

Example

```
dashboard-as-starting-page
```

Syntax

```
no dashboard-as-starting-page
```

Mode

Administration

Description

Disable to use dashboard as starting page.

Example

```
no dashboard-as-starting-page
```

Syntax

```
tls-and-above
```

Mode

Administration

Description

Enforce TLS 1.1 and above.

Example

```
tls-and-above
```

Syntax

```
no tls-and-above
```

Mode

Administration

Description

Disable enforce TLS 1.1 and above.

Example

```
no tls-and-above
```

Syntax

```
out-of-band-management
```

Mode

Administration

Description

Enable out of band management on management port.

Example

```
out-of-band-management
```

Syntax

```
no out-of-band-management
```

Mode

Administration

Description

Disable out of band management on management port.

Example

```
no out-of-band-management
```

Syntax

```
gms-management { existing-tunnel | https | ipsec-tunnel }
```

Mode

Administration

Description

Enable GMS management and set the type of tunnel to use.

Options

existing-tunnel Use existing tunnel.

https Use HTTPS.

ipsec-tunnel Use IPSEC tunnel.

Example

```
gms-management ssl
```

Syntax

```
no gms-management
```

Mode

Administration

Description

Disable GMS Management.

Example

```
no gms-management
```

Syntax

```
host-name <HOSTNAME>
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Set the GMS server IP or hostname.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
host-name 10.10.10.10
```

Syntax

no host-name

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

No set the GMS server IP or hostname.

Example

no host-name

Syntax

syslog-server-port <IPv4_PORT>

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Set the syslog server port of the GMS server.

Options

<IPv4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

syslog-server-port 514

Syntax

no syslog-server-port

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Clear syslog server port of the GMS server.

Example

no syslog-server-port

Syntax

heartbeat-status-only

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Enable Send Heartbeat Status Messages Only.

Example

```
heartbeat-status-only
```

Syntax

```
no heartbeat-status-only
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Disable Send Heartbeat Status Messages Only.

Example

```
no heartbeat-status-only
```

Syntax

```
behind-nat-device ip <IPV4_HOST>
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Enable Behind NAT Device indicator and configure IP.

Options

ip	Set IP of NAT device.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
behind-nat-device ip 192.168.168.16
```

Syntax

```
no behind-nat-device
```

Mode

GMS IPSEC
GMS Existing Tunnel
GMS HTTPS

Description

Disable Behind NAT Device indicator.

Example

```
no behind-nat-device
```

Syntax

spi <WORD>

Mode

GMS IPSEC

Description

Set Incoming / Outgoing IPSEC SPI.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

spi C50F73F4

Syntax

no spi

Mode

GMS IPSEC

Description

No set Incoming / Outgoing IPSEC SPI.

Example

no spi C50F73F4

Syntax

encryption-type des-md5

Mode

GMS IPSEC

Description

Set IPSEC encryption type.

Options

des-md5 DES-MD5.

Example

encryption-type des-md5

Syntax

encryption-key <HEX_STRING>

Mode

GMS IPSEC

Description

Set IPSEC Encryption Key.

Options

<HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

```
encryption-key 9f8c6ae4fb897002
```

Syntax

```
authentication-key <HEX_STRING>
```

Mode

GMS IPSEC

Description

Set IPSEC authentication key.

Options

<HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

```
ipsec-authentication-key bd5a1354f5a5a8e198974d4d997fac5e
```

Syntax

```
reporting-server [ ip <HOSTNAME> ] [ port <IPV4_PORT> ]
```

Mode

GMS HTTPS

Description

Enable Send Syslog Messages to a Distributed GMS Reporting Server and configure.

Options

ip Set distributed GMS reporting server IP address.
<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*
port Set distributed GMS reporting server port.
<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
reporting-server ip 10.10.10.11 port 514
```

Syntax

```
no reporting-server [ ip | port ]
```

Mode

GMS HTTPS

Description

Disable Send Syslog Messages to a Distributed GMS Reporting Server.

Options

ip Clear distributed GMS reporting server IP address.

port Clear distributed GMS reporting server port.

Example

no reporting-server

Syntax

sonicos-api

Mode

Administration

Description

SonicOS API.

Example

sonicos-api

Syntax

enable

Mode

SonicOS API

Description

Enable SonicOS API.

Example

enable

Syntax

no enable

Mode

SonicOS API

Description

Disable SonicOS API.

Example

no enable

Syntax

digest

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest access authentication.

Example

```
digest
```

Syntax

```
no digest
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest access authentication.

Example

```
no digest
```

Syntax

```
sha256-digest
```

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest SHA256.

Example

```
sha256-digest
```

Syntax

```
no sha256-digest
```

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest SHA256.

Example

```
no sha256-digest
```

Syntax

```
md5-digest
```

Mode

SonicOS API

Description

Enable SonicOS API HTTP digest MD5.

Example

md5-digest

Syntax

no md5-digest

Mode

SonicOS API

Description

Disable SonicOS API HTTP digest MD5.

Example

no md5-digest

Syntax

integrity-protection { allowed | enforced }

Mode

SonicOS API

Description

SonicOS API digest integrity protection.

Options

allowed Allowed

enforced Enforced

Example

integrity-protection allowed

Syntax

no integrity-protection

Mode

SonicOS API

Description

Disable SonicOS API digest integrity protection.

Example

no integrity-protection

Syntax

session-variant { allowed | enforced }

Mode

SonicOS API

Description

Enable SonicOS API can Use session variant.

Options

allowed Allowed

enforced Enforced

Example

session-variant allowed

Syntax

no session-variant

Mode

SonicOS API

Description

Disable SonicOS API can Use session variant.

Example

no session-variant

Syntax

chap

Mode

SonicOS API

Description

Enable SonicOS API CHAP authentication.

Example

chap

Syntax

no chap

Mode

SonicOS API

Description

Disable SonicOS API CHAP authentication.

Example

no chap

Syntax

basic

Mode

SonicOS API

Description

Enable SonicOS API HTTP basic access authentication.

Example

basic

Syntax

no basic

Mode

SonicOS API

Description

Disable SonicOS API HTTP basic access authentication.

Example

no basic

Syntax

public-key

Mode

SonicOS API

Description

Enable SonicOS API public key authentication.

Example

public-key

Syntax

no public-key

Mode

SonicOS API

Description

Disable SonicOS API public key authentication.

Example

no public-key

Syntax

rsa-key-size <UINT16>

Mode

SonicOS API

Description

SonicOS API public key RSA key size.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

rsa-key-size 1024

Syntax

rsa-padding-type { pkcsv15 | pkcsv20aep }

Mode

SonicOS API

Description

SonicOS API public key RSA padding type.

Options

pkcsv15 PKCS#1 v1.5

pkcsv20aep PKCS#1 v2.0 OAEP

Example

rsa-padding-type pkcsv20aep

Syntax

oep-hash-mode <WORD>

Mode

SonicOS API

Description

SonicOS API OEAP hashmode.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

oep-hash-mode sha1

Syntax

oep-mask-method <WORD>

Mode

SonicOS API

Description

SonicOS API OEAP mask (MGF1) method.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
oeap-mask-method sha256
```

Syntax

```
session-security
```

Mode

SonicOS API

Description

Enable SonicOS API session security.

Example

```
session-security
```

Syntax

```
no session-security
```

Mode

SonicOS API

Description

Disable SonicOS API session security.

Example

```
no session-security
```

Syntax

```
max-nonce <UINT16>
```

Mode

SonicOS API

Description

SonicOS API session security max nonce.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-nonce
```

Syntax

```
two-factor-bearer-token
```

Mode

SonicOS API

Description

Enable SonicOS API two-factor and bearer token authentication.

Example

```
two-factor-bearer-token
```

Syntax

```
no two-factor-bearer-token
```

Mode

SonicOS API

Description

Disable SonicOS API two-factor and bearer token authentication.

Example

```
no two-factor-bearer-token
```

Syntax

```
auto-commit
```

Mode

SonicOS API

Description

Enable SonicOS API auto commit.

Example

```
auto-commit
```

Syntax

```
no auto-commit
```

Mode

SonicOS API

Description

Disable SonicOS API auto commit.

Example

```
no auto-commit
```

Syntax

```
log
```

Mode

SonicOS API

Description

Enable SonicOS API log.

Example

```
log
```

Syntax

```
no log
```

Mode

SonicOS API

Description

Disable SonicOS API log.

Example

```
no log
```

Syntax

```
compress-response-during-transmission
```

Mode

SonicOS API

Description

When enabled, if the browser supported, contents larger than 1MB will compressed during transmission to optimize the speed of API response.(The downloaded content will not be compressed).

Example

```
compress-response-during-transmission
```

Syntax

```
no compress-response-during-transmission
```

Mode

SonicOS API

Description

Disable compress SonicOS API response.

Example

```
no compress-response-during-transmission
```

Syntax

```
hateoas
```

Mode

SonicOS API

Description

Enable SonicOS API HATEOAS.

Example

hateoas

Syntax

no hateoas

Mode

SonicOS API

Description

Disable SonicOS API HATEOAS.

Example

no hateoas

Syntax

force-through { any | interface <BACKEND_COMMUNICATION_INTERFACE> }

Mode

Administration

Description

Set interface to force communication with SonicWall backend servers going through.

Options

<i>any</i>	Any interface.
<i>interface</i>	Set interface.
<i><BACKEND_COMMUNICATION_INTERFACE></i>	Interface name. Example: <i>X0</i>

Example

force-through interface X1

Syntax

regenerate-certificate

Mode

Administration

Description

regenerate self-signed certificate.

Example

regenerate-certificate

Syntax

snmp

Mode

Config

Description

Enter SNMP configuration mode.

Example

```
snmp
```

Syntax

```
enable
```

Mode

SNMP

Description

Enable SNMP.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SNMP

Description

Disable SNMP.

Example

```
no enable
```

Syntax

```
system-name <WORD>
```

Mode

SNMP

Description

Set the SNMP system name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-name "Corporate Gateway"
```

Syntax

```
no system-name
```

Mode

SNMP

Description

Remove the SNMP system name.

Example

```
no system-name
```

Syntax

```
system-contact <WORD>
```

Mode

SNMP

Description

Set the SNMP system contact.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-contact "John Doe"
```

Syntax

```
no system-contact
```

Mode

SNMP

Description

Remove the SNMP system contact.

Example

```
no system-contact
```

Syntax

```
system-location <WORD>
```

Mode

SNMP

Description

Set the SNMP system location.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
system-location "Corporate Site"
```

Syntax

no system-location

Mode

SNMP

Description

Remove the SNMP system location.

Example

no system-location

Syntax

asset-number <WORD>

Mode

SNMP

Description

Set the SNMP asset number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

asset-number Unit001

Syntax

no asset-number

Mode

SNMP

Description

Remove the SNMP asset number.

Example

no asset-number

Syntax

get-community-name <WORD>

Mode

SNMP

Description

Set the SNMP get community name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
get-community-name public
```

Syntax

```
no get-community-name
```

Mode

SNMP

Description

Remove the SNMP get community name.

Example

```
no get-community-name
```

Syntax

```
trap-community-name <WORD>
```

Mode

SNMP

Description

Set the SNMP trap community name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
trap-community-name public
```

Syntax

```
no trap-community-name
```

Mode

SNMP

Description

Remove the SNMP trap community name.

Example

```
no trap-community-name
```

Syntax

```
host-1 <HOSTNAME_MIXED>
```

Mode

SNMP

Description

Set SNMP trap host 1.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

host-1 192.168.168.201

Syntax

no host-1

Mode

SNMP

Description

Remove SNMP Trap Host 1.

Example

no host-1

Syntax

host-2 <HOSTNAME_MIXED>

Mode

SNMP

Description

Set SNMP trap host 2.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

host-2 192.168.168.202

Syntax

no host-2

Mode

SNMP

Description

Remove SNMP Trap Host 2.

Example

no host-2

Syntax

host-3 <HOSTNAME_MIXED>

Mode

SNMP

Description

Set SNMP trap host 3.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

host-3 192.168.168.203

Syntax

no host-3

Mode

SNMP

Description

Remove SNMP Trap Host 3.

Example

no host-3

Syntax

host-4 <HOSTNAME_MIXED>

Mode

SNMP

Description

Set SNMP trap host 4.

Options

<HOSTNAME_MIXED> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

host-4 192.168.168.204

Syntax

no host-4

Mode

SNMP

Description

Remove SNMP Trap Host 4.

Example

```
no host-4
```

Syntax

```
snmp3 mandatory
```

Mode

SNMP

Description

Enable mandatory requirement for SNMP3.

Example

```
snmp3 mandatory
```

Syntax

```
no snmp3 mandatory
```

Mode

SNMP

Description

Disable mandatory requirement for SNMP3.

Example

```
no snmp3 mandatory
```

Syntax

```
snmp3 engine-id <WORD>
```

Mode

SNMP

Description

Set SNMP3 Engine ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
snmp3 engine-id 80002225030017C5696969
```

Syntax

```
snmp3 increase-subsystem-priority
```

Mode

SNMP

Description

Enable increase subsystem priority for SNMP3.

Example

```
snmp3 increase-subsystem-priority
```

Syntax

```
no snmp3 increase-subsystem-priority
```

Mode

SNMP

Description

Disable increase subsystem priority for SNMP3.

Example

```
no snmp3 increase-subsystem-priority
```

Syntax

```
view <SNMP_VIEW_NAME> oid <WORD>
```

Mode

SNMP

Description

Add/Edit an SNMP view OID list and enter its configuration mode.

Options

<SNMP_VIEW_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>ICMP</i>
oid	Add an OID to the SNMP view list.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
view CorpSNMPViewList oid 1.3.6.1.2.1.32
```

Syntax

```
no view <SNMP_VIEW_NAME> [ oid <SNMP_OID_IN_VIEW> ]
```

Mode

SNMP

Description

Delete an SNMP view OID list.

Options

<SNMP_VIEW_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>ICMP</i>
oid	Delete an OID from the SNMP view list.
<SNMP_OID_IN_VIEW>	SNMP view oid name. Example: <i>1.3.5</i>

Example

```
no view CorpSNMPViewList oid 1.3.6.1.2.1.32
```

Syntax

group <SNMP_GROUP_NAME>

Mode

SNMP

Description

Add an SNMP group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

group CorpSNMPGroup

Syntax

no group <SNMP_GROUP_NAME>

Mode

SNMP

Description

Delete an SNMP group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

no group CorpSNMPGroup

Syntax

name <WORD>

Mode

SNMP Group

Description

Edit an SNMP group name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name CorpSNMPGroup

Syntax

user <SNMP_USER_NAME>

Mode

SNMP

Description

Add/Edit an SNMP user and enter its configuration mode.

Options

<SNMP_USER_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
user snmp-admin1
```

Syntax

```
no user <SNMP_USER_NAME>
```

Mode

SNMP

Description

Delete an SNMP user.

Options

<SNMP_USER_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
no user snmp-admin1
```

Syntax

```
no users
```

Mode

SNMP

Description

Delete all SNMP users.

Example

```
no users
```

Syntax

```
name <WORD>
```

Mode

SNMP User

Description

Set an SNMP user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name snmp-admin1
```

Syntax

```
security-level { authentication-and-privacy | authentication-only }
```

Mode

SNMP User

Description

Set a SNMP user security level.

Options

- authentication-and-privacy** Use authentication and encryption.
- authentication-only** Use authentication.

Example

```
security-level authentication-and-privacy
security-level authentication-only
```

Syntax

```
no security-level
```

Mode

SNMP User

Description

Disable authentication and encryption.

Example

```
no security-level
```

Syntax

```
authentication { md5 <ENC_PASSWORD> | sha1 <ENC_PASSWORD> }
```

Mode

SNMP User

Description

Set a SNMP user authentication type and key.

Options

- md5** MD5.
- <ENC_PASSWORD>** Password.
Example: *secret*
- sha1** SHA-1.
- <ENC_PASSWORD>** Password.
Example: *secret*

Example

```
authentication md5 bd5a1354f5a5a8e198974d4d997fac5e
```

Syntax

```
no authentication { md5 | sha1 }
```

Mode

SNMP User

Description

Clear a SNMP user authentication type and key.

Options

md5 MD5.

sha1 SHA-1.

Example

```
no authentication md5
```

Syntax

```
encryption { aes <ENC_PASSWORD> | des <ENC_PASSWORD> }
```

Mode

SNMP User

Description

Set a SNMP user encryption.

Options

aes AES.
<ENC_PASSWORD> Password.
Example: *secret*

des DES.
<ENC_PASSWORD> Password.
Example: *secret*

Example

```
encryption des 9f8c6ae4fb897002
```

Syntax

```
no encryption { aes | des }
```

Mode

SNMP User

Description

Clear a SNMP user encryption.

Options

aes AES.

des DES.

Example

no encryption des

Syntax

group <SNMP_GROUP_NAME>

Mode

SNMP User

Description

Assign an SNMP group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

group CorpSNMPGroup

Syntax

no group

Mode

SNMP User

Description

Assign user to *No Group*.

Example

no group

Syntax

access <SNMP_ACCESS_NAME>

Mode

SNMP

Description

Add/Edit an SNMP access object and enter its configuration mode.

Options

<SNMP_ACCESS_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

access SntpAccessObject

Syntax

```
no access <SNMP_ACCESS_NAME>
```

Mode

SNMP

Description

Delete an SNMP access object.

Options

<SNMP_ACCESS_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
no access SnmpAccessObject
```

Syntax

```
no accesses
```

Mode

SNMP

Description

Delete all SNMP accesses.

Example

```
no accesses
```

Syntax

```
name <WORD>
```

Mode

SNMP Access

Description

Set an SNMP access object name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name SnmpAccessObject
```

Syntax

```
read-view <SNMP_VIEW_NAME>
```

Mode

SNMP Access

Description

Set the SNMP read view.

Options

<SNMP_VIEW_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *ICMP*

Example

```
read-view interfaces
```

Syntax

```
master-group <SNMP_GROUP_NAME>
```

Mode

SNMP Access

Description

Assign a master SNMP3 master group.

Options

<SNMP_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *Group1*

Example

```
master-group CorpSNMPGroup
```

Syntax

```
security-level { authentication-and-privacy | authentication-only }
```

Mode

SNMP Access

Description

Set SNMP access security level.

Options

authentication-and-privacy Use authentication and encryption.

authentication-only Use authentication.

Example

```
security-level authentication-only  
security-level authentication-and-privacy
```

Syntax

```
no security-level
```

Mode

SNMP Access

Description

Disable authentication and encryption.

Example

```
no security-level
```

Syntax

```
export core-dump <CORE_DUMP_NAME> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export core dump.

Options

<CORE_DUMP_NAME>	CoreDump Name. Example: <i>lastuploadedcore.gz.gpg</i>
api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: '.' -> '\\.', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export core-dump lastuploadedcore.gz.gpg scp user@server:/home/user/filename.core.zst
export core-dump lastuploadedcore.gz.gpg scp user@server:/home/user
```

Syntax

```
export swarm <WORD> { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export swarm report.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: '.' -> '\\.', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export swarm idx=0&fname=aggr12-00401034E32E-20200220025955.since.restart.wri.pdf scp user@server:/home/user/swarm_report.pdf
export swarm idx=0&fname=aggr12-00401034E32E-20200220025955.since.restart.wri.pdf scp user@server:/home/user
```

Syntax

```
export current-config { cli | exp } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

All Modes

Description

Export current configuration.

Options

cli	Export configuration using the SonicOS E-CLI command format.
exp	Export configuration using the SonicOS WebUI (.exp) format.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export current-config cli ftp ftp://user:password@servername/sw-prodname-buildversion-ecli.txt
export current-config exp scp user@server:/home/user/sw-prodname-buildversion-ecli.txt
export current-config exp scp user@server:/home/user/
```

Syntax

```
export pending-config { cli | exp } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

All Modes

Top Level

Description

Export pending configuration.

Options

cli	Export configuration using the SonicOS E-CLI command format.
exp	Export configuration using the SonicOS WebUI (.exp) format.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export pending-config cli ftp ftp://user:password@servername/sw-prodname-buildversion-ecli.txt
export pending-config cli scp user@server:/home/user/sw-prodname-buildversion-ecli.txt
export pending-config cli scp user@server:/home/user/
```

Syntax

```
export tech-support-report { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export the technical support report.

Options

ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export tech-support-report ftp ftp://user:password@servername/techSupport.wri
export tech-support-report scp user@server:/home/user/techSupport.wri
export tech-support-report scp user@server:/home/user
```

Syntax

```
export ssoauth-log { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export SSO AUTH log.

Options

api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export ssoauth-log ftp ftp://user:password@servername/ssoauthLog.log
export ssoauth-log scp user@server:/home/user/ssoauthLog.log
export ssoauth-log scp user@server:/home/user
```

Syntax

```
export-and-reset ssoauth-log { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export and reset SSO AUTH log.

Options

api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export-and-reset ssoauth-log ftp ftp://user:password@servername/ssoauthLog.log
export-and-reset ssoauth-log scp user@server:/home/user/ssoauthLog.log
export-and-reset ssoauth-log scp user@server:/home/user
```

Syntax

```
export trace-log <WORD> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export trace log.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export trace-log &traceLogType=1 scp user@server:/home/user/tracelog.wri
export trace-log &traceLogType=1 scp user@server:/home/user
```

Syntax

```
export console-logs { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export console logs.

Options

api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export console-logs scp user@server:/home/user/consolelogs.wri
export console-logs scp user@server:/home/user
```

Syntax

```
export safe-mode-logs { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export safe-mode logs.

Options

api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export safe-mode-logs scp user@server:/home/user/safemodelogs.wri
export safe-mode-logs scp user@server:/home/user
```

Syntax

```
export object { actions | address-objects | applications | country-objects | custom-matches | services | threat-prevention-  
profiles | url-list | web-categories }
```

Mode

Top Level
Config

Description

export specified objects.

Options

actions	action object.
address-objects	address object.
applications	application object.
country-objects	country object.
custom-matches	custom-match object.
services	service object.
threat-prevention-profiles	threat prevention profile.
url-list	url-list object.
web-categories	web category object.

Example

```
export object address-objects
```

Syntax

```
export policy { decryption-policies | dos-policies | nat-policies | route-policies | security-policies }
```

Mode

Top Level
Config

Description

export specified policies.

Options

decryption-policies	export decryption policies
dos-policies	export dos policies
nat-policies	export nat policies
route-policies	export route policies
security-policies	export security policies

Example

```
export policy security-policies
```

Syntax

```
export shadow-rule-list { access-rules | decryption-policies | dos-policies | nat-policies | route-policies }
```

Mode

Top Level
Config

Description

export specified shadow rule list by api.

Options

<i>access-rules</i>	export security policies shadow rule list
<i>decryption-policies</i>	export decryption policies shadow rule list
<i>dos-policies</i>	export dos policies shadow rule list
<i>nat-policies</i>	export nat policies shadow rule list
<i>route-policies</i>	export route policies shadow rule list

Example

```
export shadow-rule-list security-policies
```

Syntax

```
export firmware { current | system-backup | uploaded } { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export the current firmware.

Options

<i>current</i>	Export current firmware.
<i>system-backup</i>	Export system-backup firmware.
<i>uploaded</i>	Export uploaded firmware.
<i>api</i>	Export using the api.
<i>ftp</i> <FTP_URL>	Export using the FTP protocol. FTP URL in the form: ftp://username:password@hostname/ Escape character: '!' -> '\\!', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/
<i>scp</i> <SCP_URL>	Export using the SCP protocol. SCP URL in the form: userName@serverip:/fileDirectory. Example: userTest@10.10.10.10:/home/userTest/
<i>port</i> <IPV4_PORT>	SCP server port Integer in the form: D OR 0xHHHH. Example: 80

Example

```
export current firmware scp user@server:/home/user/firmware.bin.sig  
export current firmware scp user@server:/home/user
```

Syntax

```
firmware auto { download | update }
```

Mode

Config

Description

Enable periodic checking of SonicWall site for firmware update.

Options

download Enable automatic downloading of firmware from SonicWall software site.

update Enable periodic checking of SonicWall site for firmware update.

Example

```
firmware auto update
```

Syntax

```
no firmware auto { download | update }
```

Mode

Config

Description

Disable periodic checking of SonicWall site for firmware update.

Options

download Disable automatic downloading of firmware from SonicWall software site.

update Disable periodic checking of SonicWall site for firmware update.

Example

```
no firmware auto update
```

Syntax

```
ftp send-tsrf
```

Mode

Config

Description

Enable send tech support report by FTP.

Example

```
ftp send-tsrf
```

Syntax

```
no ftp send-tsrf
```

Mode

Config

Description

Disable send tech support report by FTP.

Example

```
no ftp send-tsrf
```

Syntax

```
ftp send-settings
```

Mode

Config

Description

Enable send settings by FTP.

Example

```
ftp send-settings
```

Syntax

```
no ftp send-settings
```

Mode

Config

Description

Disable send settings by FTP.

Example

```
no ftp send-settings
```

Syntax

```
ftp server <IPV4_HOST>
```

Mode

Config

Description

Set FTP sever.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
ftp server 192.168.168.168
```

Syntax

```
no ftp server
```

Mode

Config

Description

Clear FTP sever.

Example

```
no ftp server
```

Syntax

```
ftp user <WORD>
```

Mode

Config

Description

Set FTP user.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp user test
```

Syntax

```
no ftp user
```

Mode

Config

Description

Clear FTP user.

Example

```
no ftp user
```

Syntax

```
ftp password <ENC_PASSWORD>
```

Mode

Config

Description

Set FTP password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
ftp password mypassword
```

Syntax

no ftp password

Mode

Config

Description

Clear FTP password.

Example

no ftp password

Syntax

ftp directory <WORD>

Mode

Config

Description

Set FTP directory.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ftp directory root

Syntax

no ftp directory

Mode

Config

Description

Clear FTP directory.

Example

no ftp directory

Syntax

no upload-firmware

Mode

Config

Description

Delete uploaded firmware.

Example

no upload-firmware

Syntax

no local-backups version <WORD>

Mode

Config

Description

Delete this backup firmware and all configurations.

Options

- version** Local backup firmware version.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no local-backups version local_fw_backup_ver_12345678

Syntax

local-backups boot version <WORD>

Mode

Config

Description

Boot local backup firmware with factory default configuration.

Options

- version** Local backup firmware version.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

local-backups boot version local_fw_backup_ver_12345678

Syntax

local-backup create { no-retain | retain } comment [<WORD>]

Mode

Config

Description

Create local backup.

Options

- no-retain** set local backup is not retain.
- retain** set local backup retain.
- comment** Set local backup comment.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
local-backup create no-retain comment backup_comment
```

Syntax

```
no local-backup name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Delete local backup.

Options

<LOCAL_BACKUP_NAME> Local backup name.
Example: *abc*

Example

```
no local-backup sonicwall-20200106010550-20200202073202
```

Syntax

```
local-backup comment <WORD> name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Edit local backup comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

name local backup name.

<LOCAL_BACKUP_NAME> Local backup name.
Example: *abc*

Example

```
local-backup comment test_comment name sonicwall-20200106010550-20200202073202
```

Syntax

```
no local-backup comment name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Clear local backup comment.

Options

name local backup name.

<LOCAL_BACKUP_NAME> Local backup name.
Example: *abc*

Example

```
no local-backup comment name sonicwall-20200106010550-20200202073202
```

Syntax

```
local-backup retain name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Set local backup retain.

Options

<i>name</i>	local backup name.
<i><LOCAL_BACKUP_NAME></i>	Local backup name. Example: <i>abc</i>

Example

```
local-backup retain name sonicwall-20200106010550-20200202073202
```

Syntax

```
no local-backup retain name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Unset local backup retain.

Options

<i>name</i>	local backup name.
<i><LOCAL_BACKUP_NAME></i>	Local backup name. Example: <i>abc</i>

Example

```
no local-backup retain name sonicwall-20200106010550-20200202073202
```

Syntax

```
local-backup gold name <LOCAL_BACKUP_NAME>
```

Mode

Config

Description

Set local backup favorite.

Options

<i>name</i>	local backup name.
<i><LOCAL_BACKUP_NAME></i>	Local backup name. Example: <i>abc</i>

Example

```
local-backup gold name sonicwall-20200106010550-20200202073202
```

Syntax

no local-backup gold name <LOCAL_BACKUP_NAME>

Mode

Config

Description

Unset local backup favorite.

Options

- name** local backup name.
- <LOCAL_BACKUP_NAME>** Local backup name.
Example: *abc*

Example

no local-backup gold name sonicwall-20200106010550-20200202073202

Syntax

no cloud-backups version <CLOUD_BACKUP_FIRMWARE_NAME>

Mode

Config

Description

Delete all cloud backup configurations with specific firmware version.

Options

- version** Cloud backup firmware version.
- <CLOUD_BACKUP_FIRMWARE_NAME>** Cloud backup name.
Example: *abc*

Example

no cloud-backups version cloud_fw_backup_ver_12345678

Syntax

cloud-backup create { no-retain | retain } comment [<WORD>]

Mode

Config

Description

Create cloud backup.

Options

- no-retain** Do not Retain Cloud Backup.
- retain** Retain Cloud Backup.
- comment** Set cloud backup comment.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

cloud-backup create

Syntax

no cloud-backup name <WORD>

Mode

Config

Description

Delete cloud backup.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

no cloud-backup name pref_backup_12345678

Syntax

cloud-backup retain name <WORD>

Mode

Config

Description

Set cloud backup retain.

Options

name Cloud backup name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

cloud-backup name pref_backup_12345678 retain

Syntax

no cloud-backup retain name <WORD>

Mode

Config

Description

Set cloud backup no retain.

Options

name Cloud backup name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

no cloud-backup name pref_backup_12345678 retain

Syntax

no cloud-backup comment name <WORD>

Mode

Config

Description

Clear cloud backup comment.

Options

- name*** Cloud backup name.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no cloud-backup comment name pref_backup_12345678

Syntax

cloud-backup comment <WORD> name <WORD>

Mode

Config

Description

Edit cloud backup comment.

Options

- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- name*** Cloud backup name.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

cloud-backup name pref_backup_12345678 coment test

Syntax

cloud-backup gold name <WORD>

Mode

Config

Description

Set cloud backup favotite.

Options

- name*** cloud backup name.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

cloud-backup gold name pref_cloud_backup_123456

Syntax

no cloud-backup gold name <WORD>

Mode

Config

Description

Unset cloud backup favorite.

Options

- name** cloud backup name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no cloud-backup gold name pref_cloud_backup_123456

Syntax

auto-upgrade

Mode

Config
Top Level

Description

Proceed auto-upgrade firmware.

Example

auto-upgrade

Syntax

no auto-upgrade

Mode

Config
Top Level

Description

cancel auto-upgrade firmware.

Example

no auto-upgrade

Syntax

import firmware { api | ftp <FTP_URL> | scp <SCP_URL> [port <IPV4_PORT>] }

Mode

Config

Description

Import firmware to the firewall.

Options

- api** Import using the api.

ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPv4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import firmware ftp ftp://user:password@servername/soniccore-sonicos-xxx.swi
import firmware scp user@server:/home/user/soniccore-sonicos-xxx.swi
```

Syntax

```
import cli { { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPv4_PORT> ] } | terminal } merge [ best-effort ] [ clear-pending ]
```

Mode

Config

Description

Import configuration using the SonicOS E-CLI command format.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPv4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
terminal	Import using the terminal.
merge	Combines configuration imported with the current configuration running and saved to the device.
best-effort	Ignore validation errors and import only valid configuration (best effort).
clear-pending	Clear pending changes.

Example

```
import cli terminal
```

Syntax

```
import exp { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPv4_PORT> ] }
```

Mode

Config

Description

Import configuration using the SonicOS WebUI (.exp) format.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPv4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import exp ftp ftp://user:password@servername/soniccore-sonicos-xxx.swi
import exp scp user@server:/home/user/soniccore-sonicos-xxx.swi
```

Syntax

```
get <WORD> [ qs <WORD> ] [ body { json | multipart | text } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPv4_PORT> ] } ]
```

Mode

Import Api

Description

Import api get commands.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
qs	Api query string.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
body	Api body.
json	Application/json format.
multipart	multipart format.
text	Text/plain format.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPv4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
get api/sonicos/administration/global
```

Syntax

```
put <WORD> [ qs <WORD> ] [ body { json | multipart | text } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPv4_PORT> ] } ]
```

Mode

Import Api

Description

Import api put commands.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
qs	Api query string.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
body	Api body.
json	Application/json format.
multipart	multipart format.
text	Text/plain format.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
put api/sonicos/administration/global body ftp ftp://user:password@servername/xxx
```

Syntax

```
post <WORD> [ qs <WORD> ] [ body { json | multipart | text } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] } ]
```

Mode

Import Api

Description

Import api post commands.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
qs	Api query string.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
body	Api body.
json	Application/json format.
multipart	multipart format.
text	Text/plain format.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
post api/sonicos/address-objects/ipv4 body ftp ftp://user:password@servername/xxx
```

Syntax

```
delete <WORD> [ qs <WORD> ] [ body { json | multipart | text } { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] } ]
```

Mode

Import Api

Description

Import api delete commands.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
qs	Api query string.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
body	Api body.
json	Application/json format.
multipart	multipart format.
text	Text/plain format.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
delete api/sonicos/address-objects/ipv4/name/xxx
```

Syntax

```
import file { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Import Api

Description

Import api commands from file.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
import file ftp ftp://user:password@servername/xxx
```

Syntax

```
restart [ at <TIME_YYYYMMDDHHMMSS> | cancel | in <UINT32> { days | hours | minutes } | now | time <UINT32> ]
```

Mode

Top Level
Config

Description

Restart SonicOS - now or after an interval of time.

Options

at	Restart at the time specified.
<TIME_YYYYMMDDHHMMSS>	Timestamp in the form: YYYY:MM:DD:HH:MM:SS. Example: <i>2010:06:30:23:30:59</i>
cancel	Cancel restart.
in	Restart after the specified interval.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
days	Set in days.
hours	Set in hours.
minutes	Set in minutes.
now	Restart immediately.
time	Restart after the specified number of seconds.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
restart
```

Syntax

```
safemode
```

Mode

Top Level

Description

Restart the device and enter safemode.

Example

```
safemode
```

Syntax

restore-defaults

Mode

Config

Description

Restore the device to factory default settings.

Example

restore-defaults

Syntax

boot { { { current | uploaded } [factory-default] } | cloud-backup <WORD> | local-backup <LOCAL_BACKUP_NAME> [delay <UINT16>] }

Mode

Config

Description

Boot current or uploaded firmware image with current or default settings or boot system backup.

Options

<i>current</i>	Boot current firmware image.
<i>uploaded</i>	Boot the latest uploaded firmware image.
<i>factory-default</i>	Boot current firmware with default settings.
<i>cloud-backup</i> <WORD>	Boot cloud backup with specified preference. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>local-backup</i> <LOCAL_BACKUP_NAME>	local backup. Local backup name. Example: <i>abc</i>
<i>delay</i> <UINT16>	Reboot system after the specified interval Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

boot current factory-default

Syntax

sysfile

Mode

Config

Description

sysfile operation.

Example

sysfile

Syntax

```
storage-dev <UINT8>
```

Mode

SYSFILE

Description

Set storage dev by devId.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
storage-dev 1
```

Syntax

```
logs-on-storage
```

Mode

SYSFILE

Description

Enable log files on storage.

Example

```
logs-on-storage
```

Syntax

```
no logs-on-storage
```

Mode

SYSFILE

Description

Disable log files on storage.

Example

```
no logs-on-storage
```

Syntax

```
clear sysfile { config | diagdata | log | sysdata } <WORD> dev <INT32>
```

Mode

SYSFILE

Description

Delete log file on device.

Options

config Specify configuration backup

diagdata Specify diagnostic data

log	Specify logs
sysdata	Specify system data
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
dev	Specify device
<INT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
clear sysfile { log | sysdata | diagdata | config } "abc" dev 1
```

Syntax

```
no connection caches
```

Mode

Top Level
Config

Description

clear all connection cache elements.

Example

```
no connection caches
```

Syntax

```
no connection cache src-ip <WORD> src-port <UINT32> dst-ip <WORD> dst-port <UINT32> proto <WORD> src-inf <WORD> dst-inf <WORD>
dst-nat <UINT32>
```

Mode

Top Level
Config

Description

clear connection cache element.

Options

src-ip	Source Ip
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
src-port	Source Port
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
dst-ip	Dstination Ip
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
dst-port	Dstination Port
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
proto	Protocal
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
src-inf	Source Interface
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
dst-inf	Destination Interface
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
dst-nat	Destination NAT
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
no connection cache src-ip 10.21.49.241 src-port 55789 dst-ip 10.21.49.12 dst-port 443 proto TCP src-inf X1 dst-inf X2 dst-nat 27
```

Syntax

```
export sysfile { config | diagdata | log dev <INT32> | sysdata } { csv | txt } <WORD> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export sysfile log in csv or txt format.

Options

config	configuration backup file.
diagdata	diagdata file.
log	log file.
dev	Specify device
<INT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
sysdata	sysdata file.
csv	CSV format.
txt	Text format.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: abc
api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: userTest@10.10.10.10:/home/userTest/
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: 80

Example

```
export sysfile log dev 0 csv eventlog.csv ftp ftp://user:password@servername/log.csv
export sysfile log dev 0 csv eventlog.csv scp user@server:/home/user/log.csv
export sysfile log dev 0 csv eventlog.csv scp user@server:/home/user/
```

Syntax

time

Mode

Config

Description

Enter time configuration mode.

Example

time

Syntax

time <TIME_HHMMSS>

Mode

Time

Description

Specify time.

Options

<TIME_HHMMSS> Time in the form: DD:DD:DD.
Example: *12:00:00*

Example

time 12:30:59

Syntax

date <DATE_YYYYMMDD>

Mode

Time

Description

Specify date.

Options

<DATE_YYYYMMDD> Date in the form: YYYY:MM:DD.
Example: *2010:06:30*

Example

date 2010:06:31

Syntax

time-zone <TIME_ZONE>

Mode

Time

Description

Specify time zone.

Options

<TIME_ZONE> Time Zone.
Example: *pacific-time*

Example

time-zone pacific-time
time-zone atlantic-time

```
time-zone russia-gmt+7
time-zone china,philippines
```

Syntax

```
use-ntp
```

Mode

Time

Description

Enable use of NTP servers to obtain time.

Example

```
use-ntp
```

Syntax

```
no use-ntp
```

Mode

Time

Description

Disable use of NTP servers to obtain time.

Example

```
no use-ntp
```

Syntax

```
daylight-savings
```

Mode

Time

Description

Enable automatic adjustment of clock for daylight saving time.

Example

```
daylight-savings
```

Syntax

```
no daylight-savings
```

Mode

Time

Description

Disable automatic adjustment of clock for daylight saving time.

Example

```
no daylight-savings
```

Syntax

universal

Mode

Time

Description

Enable display of UTC in logs (instead of local time).

Example

universal

Syntax

no universal

Mode

Time

Description

Disable display of UTC in logs (instead of local time).

Example

no universal

Syntax

international-format

Mode

Time

Description

Enable display of date in international format.

Example

international-format

Syntax

no international-format

Mode

Time

Description

Disable display of date in international format.

Example

no international-format

Syntax

only-custom-ntp

Mode

Time

Description

Enable only use custom NTP servers.

Example

only-custom-ntp

Syntax

no only-custom-ntp

Mode

Time

Description

Disable only use custom NTP servers.

Example

no only-custom-ntp

Syntax

ntp-update-interval <UINT16>

Mode

Time

Description

Set the NTP Update Interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

ntp-update-interval 123

Syntax

ntp-server <NTP_SERVER>

Mode

Time

Description

Add a server to the NTP server list.

Options

<NTP_SERVER> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
ntp-server 192.168.168.160
ntp-server 2016:12:15::2016
```

Syntax

```
no ntp-server <NTP_SERVER>
```

Mode

Time

Description

Remove a server from the NTP server list.

Options

<NTP_SERVER> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
no ntp-server 192.168.168.160
```

Syntax

```
no ntp-servers
```

Mode

Time

Description

Remove all servers from the NTP server list.

Example

```
no ntp-servers
```

Syntax

```
name <NTP_SERVER>
```

Mode

NTP server

Description

Edit NTP server name.

Options

<NTP_SERVER> IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
name 192.168.168.160
name 2016:12:15::2016
```

Syntax

no-auth

Mode

NTP server

Description

NTP server doesn't require authentication.

Example

no-auth

Syntax

md5 trust-key-no <UINT16> key-number <UINT16> password <ENC_PASSWORD>

Mode

NTP server

Description

NTP server uses MD5 authentication.

Options

<i>trust-key-no</i>	Trust key.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>key-number</i>	Key number.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>password</i>	Password.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>

Example

md5 trust-key-no 10 key-number 20 password password

Syntax

license

Mode

Config

Description

License configuration.

Example

license

Syntax

synchronize

Mode

License

Description

Synchronize licenses with www.mysonicwall.com.

Example

synchronize

Syntax

lmsync

Mode

License

Description

Synchronize licenses with license manager.

Example

lmsync

Syntax

upgrade { [key <WORD>] [key-set <WORD>] }

Mode

License

Description

Manual upgrade services.

Options

- key** Upgrade by key.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- key-set** Upgrade by key set.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

upgrade key CARZFDMR

Syntax

register-code <WORD>

Mode

License

Description

Set the register code.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

register-code 955SG6SE

Syntax

ssh server

Mode

Config

Description

Enter SSH server configuration mode.

Example

ssh server

Syntax

port <IPV4_PORT>

Mode

SSH Server

Description

Set the SSH port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 4022

Syntax

keygen

Mode

SSH Server

Description

Generate authentication keys for SSH.

Example

keygen

Syntax

restart

Mode

SSH Server

Description

Restart SSH server.

Example

restart

Syntax

enable

Mode

SSH Server

Description

Enable SSH server.

Example

enable

Syntax

terminate

Mode

SSH Server

Description

Disable SSH access and terminate all SSH sessions.

Example

terminate

Syntax

kill session ip <SSH_SERVER_SESSION_IP> port <SSH_SERVER_SESSION_PORT>

Mode

SSH Server

Description

Terminate specified SSH session.

Options

<i>ip</i>	Terminate session at specified ip.
<i><SSH_SERVER_SESSION_IP></i>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
<i>port</i>	Client port.
<i><SSH_SERVER_SESSION_PORT></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

kill session ip 192.168.168.12 port 52781

Syntax

kill sessions

Mode

SSH Server

Description

Terminate all SSH session.

Example

```
kill sessions
```

Syntax

```
fips
```

Mode

Config

Description

Enable FIPS mode.

Example

```
fips
```

Syntax

```
no fips
```

Mode

Config

Description

Disable FIPS mode.

Example

```
no fips
```

Syntax

```
ndpp
```

Mode

Config

Description

Enable NDPP mode.

Example

```
ndpp
```

Syntax

```
no ndpp
```

Mode

Config

Description

Disable NDPP mode.

Example

```
no ndpp
```

Syntax

```
show administration [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Administration Configuration and Information.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show administration
```

Syntax

```
show snmp [ access <SNMP_ACCESS_NAME> | accesses | base | group <SNMP_GROUP_NAME> | groups | user <SNMP_USER_NAME> | users | views ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SNMP Configuration and Information.

Options

<i>access</i> <SNMP_ACCESS_NAME>	Show a specified SNMP access configuration. Word in the form: WORD or \"QUOTED STRING\". Example: <i>Group1</i>
<i>accesses</i>	Show SNMP accesses configuration.
<i>base</i>	Show SNMP base settings.
<i>group</i> <SNMP_GROUP_NAME>	Show a specified SNMP group configuration. Word in the form: WORD or \"QUOTED STRING\". Example: <i>Group1</i>
<i>groups</i>	Show SNMP groups configuration.
<i>user</i> <SNMP_USER_NAME>	Show a specified SNMP user configuration. Word in the form: WORD or \"QUOTED STRING\". Example: <i>Group1</i>
<i>users</i>	Show SNMP users configuration.
<i>views</i>	Show SNMP views configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

show snmp

Syntax

```
show firmware [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Firmware configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show firmware
```

Syntax

```
show ftp [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show ftp configuration.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show ftp
```

Syntax

```
show status [ interfaces | security-services | storage | system ]
```

Mode

All Modes

Description

Show basic system status and information.

Options

interfaces Show network interfaces status.

security-services Show security services status.

<i>storage</i>	Show storage status.
<i>system</i>	Show system infomation.

Example

```
show status
```

Syntax

```
show sysfile [ configbk | diagdata | log | storage | sysdata ]
```

Mode

All Modes

Description

Show sysfile storage.

Options

<i>configbk</i>	Show configuration backup files.
<i>diagdata</i>	Show diagnostic data files.
<i>log</i>	Show log files.
<i>storage</i>	Show storage configuration.
<i>sysdata</i>	Show system data files.

Example

```
show sysfile
```

Syntax

```
show time [ base | ntp-server <NTP_SERVER> | ntp-servers ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Time settings or NTP settings.

Options

<i>base</i>	Show Time base settings.
<i>ntp-server</i> <NTP_SERVER>	Show a specific NTP server settings. IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n
<i>ntp-servers</i>	Show all NTP servers settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show time
```

Syntax

show version

Mode

All Modes

Syntax

show license [{ pending-config | with-pending-config } | [security-services] status]

Mode

All Modes

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>security-services</i>	Show license security services status.
<i>status</i>	Show license status.

Syntax

show ssh server [{ pending-config | with-pending-config } | sessions]

Mode

All Modes

Description

Show SSH server configuration.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>sessions</i>	Show SSH server sessions.

Example

show ssh server

Syntax

show fips [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show FIPS configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show fips
```

Syntax

```
show ndpp [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show NDPP configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show ndpp
```

Syntax

```
user authentication
```

Mode

Config

Description

Configure user authentication related settings.

Example

```
user authentication
```

Syntax

```
auth-method { ldap | ldap-local | local | radius | radius-local | tacacs | tacacs-local }
```

Mode

User Authentication

Description

Set the user authentication method.

Options

- ldap*** Use LDAP user authentication.

<i>ldap-local</i>	Use both LDAP and local user authentication.
<i>local</i>	Use local user authentication.
<i>radius</i>	Use RADIUS user authentication.
<i>radius-local</i>	Use both RADIUS and local user authentication.
<i>tacacs</i>	Use TACACS+ user authentication.
<i>tacacs-local</i>	Use both TACACS+ and local user authentication.

Example

```
method local
```

Syntax

```
sso-method { browser-ntlm [ { after-sso-agent-failed | before-sso-agent | enabled } ] | capture-client | radius-accounting | sso-agent | terminal-services-agent | third-party-api }
```

Mode

User Authentication

Description

Enable the single-sign-on mechanism.

Options

<i>browser-ntlm</i>	Enable browser NTLM authentication.
<i>after-sso-agent-failed</i>	Use NTLM to authenticate HTTP traffic only if SSO via the agent fails.
<i>before-sso-agent</i>	Use NTLM to authenticate HTTP traffic before attempting SSO via the agent.
<i>enabled</i>	Enable browser-ntlm option.
<i>capture-client</i>	Enable capture client authentication.
<i>radius-accounting</i>	Enable RADIUS accounting authentication.
<i>sso-agent</i>	Enable SSO agent authentication.
<i>terminal-services-agent</i>	Enable terminal services agent authentication.
<i>third-party-api</i>	Enable third party api authentication.

Example

```
sso-method sso-agent
```

Syntax

```
no sso-method { browser-ntlm | capture-client | radius-accounting | sso-agent | terminal-services-agent | third-party-api }
```

Mode

User Authentication

Description

Disable the single-sign-on mechanism.

Options

<i>browser-ntlm</i>	Disable browser NTLM authentication.
<i>capture-client</i>	Enable capture client authentication.
<i>radius-accounting</i>	Disable RADIUS accounting authentication.
<i>sso-agent</i>	Disable SSO agent authentication.
<i>terminal-services-agent</i>	Disable terminal services agent authentication.
<i>third-party-api</i>	Enable third party api authentication.

Example

```
no sso-method sso-agent
```

Syntax

```
case-sensitive-names
```

Mode

User Authentication

Description

Enable treating user names as case-sensitive.

Example

```
case-sensitive-names
```

Syntax

```
no case-sensitive-names
```

Mode

User Authentication

Description

Disable treating user names as case-sensitive.

Example

```
no case-sensitive-names
```

Syntax

```
login-uniqueness
```

Mode

User Authentication

Description

Enable enforcing a single login per user name.

Example

```
login-uniqueness
```

Syntax

no login-uniqueness

Mode

User Authentication

Description

Disable enforcing a single login per user name.

Example

no login-uniqueness

Syntax

relogin-after-password-change

Mode

User Authentication

Description

Enable enforcing relogin after password change.

Example

relogin-after-password-change

Syntax

no relogin-after-password-change

Mode

User Authentication

Description

Disable enforcing relogin after password change.

Example

no relogin-after-password-change

Syntax

display-login-info

Mode

User Authentication

Description

Display user login info since last login.

Example

display-login-info

Syntax

no display-login-info

Mode

User Authentication

Description

Disable display user login info since last login.

Example

no relogin-after-password-change

Syntax

one-time-password-constraints

Mode

User Authentication

Description

Enable One Time Password constraints.

Example

one-time-password-constraints

Syntax

no one-time-password-constraints

Mode

User Authentication

Description

Disable One Time Password constraints.

Example

no one-time-password-constraints

Syntax

one-time-password format { characters | mixed | numbers }

Mode

User Authentication

Description

Set one-time password format.

Options

characters Characters format.

mixed Mixed format.

numbers Numbers format.

Example

one-time-password format characters

Syntax

```
one-time-password length { [ min <UINT8> ] [ max <UINT8> ] }
```

Mode

User Authentication

Description

Set one-time password length.

Options

<i>min</i>	Minimum length.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>max</i>	Maximum length.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

```
one-time-password length min 8 max 12
```

Syntax

```
one-time-password email-format { html | plain-text }
```

Mode

User Authentication

Description

Set one-time password e-mail format.

Options

<i>html</i>	Html format.
<i>plain-text</i>	Plain-text format.

Example

```
one-time-password email-format html
```

Syntax

```
auth-page-timeout <UINT16>
```

Mode

User Authentication

Description

Set the timeout for showing the web login page.

Options

<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
auth-page-timeout 2
```

Syntax

no auth-page-timeout

Mode

User Authentication

Description

Clear the timeout for showing the web login page.

Example

no auth-page-timeout

Syntax

browser-redirect-via { host-name | interface-ip | name-from-certificate | reverse-dns }

Mode

User Authentication

Description

Set the method for redirect the browser to this appliance.

Options

<i>host-name</i>	Redirect the browser via domain name configured for firewall.
<i>interface-ip</i>	Redirect the browser via the interface ip address.
<i>name-from-certificate</i>	Redirect the browser via name from the administration certificate.
<i>reverse-dns</i>	Redirect the browser via domain name from a reverse DNS lookup of the interface IP address.

Example

browser-redirect-via interface-ip

Syntax

redirect-to-login-page { directly | via-info-page }

Mode

User Authentication

Description

Set the method for redirect the browser to this appliance.

Options

<i>directly</i>	Redirect users to login page directly.
<i>via-info-page</i>	Redirect users to login page via informatory intermdiate page.

Example

redirect-to-login-page directly

Syntax

```
http-redirect-after-login
```

Mode

User Authentication

Description

Enable redirect from HTTPS to HTTP after login.

Example

```
http-redirect-after-login
```

Syntax

```
no http-redirect-after-login
```

Mode

User Authentication

Description

Disable redirect from HTTPS to HTTP after login.

Example

```
no http-redirect-after-login
```

Syntax

```
radius-chap-http-login
```

Mode

User Authentication

Description

Enable allowing HTTP login with RADIUS CHAP mode when that is available rather than redirecting to HTTPS for web login.

Example

```
radius-chap-http-login
```

Syntax

```
no radius-chap-http-login
```

Mode

User Authentication

Description

Disable allowing HTTP login with RADIUS CHAP mode when that is available rather than redirecting to HTTPS for web login.

Example

```
no radius-chap-http-login
```

Syntax

```
redirect-external-page <WORD>
```

Mode

User Authentication

Description

Redirect to the specified external login page on redirecting unauthenticated users.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
externalPage www.aaa.com
```

Syntax

```
no redirect-external-page
```

Mode

User Authentication

Description

Disable redirect to external login page on redirecting unauthenticated users.

Example

```
no redirect-external-page
```

Syntax

```
combined-login { enable | http }
```

Mode

User Authentication

Description

Enable authenticate user's other IP(V4/V6) addresses if possible or use http to initiate combined logins.

Options

enable Enable authenticate user's other IP(V4/V6) addresses if possible.

http Enable use HTTP to initiate combined logins.

Example

```
combined-login enable  
combined-login http
```

Syntax

```
no combined-login { enable | http }
```

Mode

User Authentication

Description

Disable authenticate user's other IP(V4/V6) addresses if possible or http to initiate combined logins.

Options

enable Enable authenticate user's other IP(V4/V6) addresses if possible.

http Disable use HTTP to initiate combined logins.

Example

```
no combined-login enable
no combined-login http
```

Syntax

```
auth-page-as-frame
```

Mode

User Authentication

Description

Enable allow authentication page in frame.

Example

```
auth-page-as-frame
```

Syntax

```
no auth-page-as-frame
```

Mode

User Authentication

Description

Disable allow authentication page in frame.

Example

```
no auth-page-as-frame
```

Syntax

```
policy-banner-before-login
```

Mode

User Authentication

Description

Enable start with policy banner before login page.

Example

```
policy-banner-before-login
```

Syntax

```
no policy-banner-before-login
```

Mode

Description

Clear start with policy banner before login page.

Example

```
no policy-banner-before-login
```

Syntax

```
policy-banner content <ROL>
```

Mode

User Authentication

Description

Set the policy banner displayed to users before login.

Options

content	Set the content for the policy banner.
<ROL>	Remaining command line input. Example: <i>line...</i>

Example

```
policy-banner
```

Syntax

```
no policy-banner content
```

Mode

User Authentication

Description

Clear the policy banner displayed to users before login.

Options

content	Clear the policy banner content.

Example

```
no policy-banner content
```

Syntax

```
inactivity-timeout <UINT16>
```

Mode

User Authentication

Description

Set the user inactivity timeout(minutes).

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
inactivity-timeout 60
```

Syntax

```
prevent-inactivity-logout service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

User Authentication

Description

Set service to prevent user logout on inactivity.

Options

group	Service group.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
prevent-inactivity-logout service name FTP
```

Syntax

```
no prevent-inactivity-logout service
```

Mode

User Authentication

Description

Clear service of traffic to prevent user logout on inactivity.

Example

```
no prevent-inactivity-logout service
```

Syntax

```
log-user-name { bypass-sso <WORD> | originating-externally <WORD> | other-unidentified <WORD> | sso-fail <WORD> }
```

Mode

User Authentication

Description

Set user name for logging of connections on which the user is not identified.

Options

bypass-sso	For connections that bypass SSO.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
originating-externally	For connections originating externally.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
other-unidentified	For other unidentified connections.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
sso-fail	If SSO fails to identify the user.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
log-user-name originating-externally oriExternUser
```

Syntax

```
no log-user-name { bypass-sso | originating-externally | other-unidentified | sso-fail }
```

Mode

User Authentication

Description

Set no user name for logging of connections on which the user is not identified.

Options

bypass-sso	For connections that bypass SSO.
originating-externally	Set no user name for connections originating externally.
other-unidentified	Set no user name for other unidentified
sso-fail	If SSO fails to identify the user.

Example

```
no log-user-name originating-externally
```

Syntax

```
user-connections-logout { inactivity | reported } { authentication | other } { keep-alive | terminate [ after <UINT16> | now ] }
```

Mode

User Authentication

Description

Set activity for any remaining user connections on logout.

Options

inactivity	Set activity for any remaining user connections on logout due to inactivity.
reported	Set activity for any remaining user connections on active/reported logout.

<i>authentication</i>	Set activity for authentication connections.
<i>other</i>	Set activity for other connections.
<i>keep-alive</i>	Leave the connections alive.
<i>terminate</i>	Terminate the connections.
<i>after</i>	Terminate the connections after specified minutes.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>now</i>	Terminate the connections now.

Example

```
user-connections-logout inactivity authentication keep-alive
user-connections-logout inactivity other terminate
user-connections-logout inactivity other terminate after 15
```

Syntax

```
inactive-user { login | timeout }
```

Mode

User Authentication

Description

Enable make user into an inactive state.

Options

- login*** Enable make the user initially inactive until they send traffic on being notified of a login.
- timeout*** Enable make all users inactive instead of logging out on inactivity timeout.

Example

```
inactive-user login
```

Syntax

```
no inactive-user { login | timeout }
```

Mode

User Authentication

Description

Disable make user into an inactive state.

Options

- login*** Disable make the user initially inactive until they send traffic on being notified of a login.
- timeout*** Disable make all users inactive instead of logging out on inactivity timeout.

Example

```
no inactive-user login
```

Syntax

age-out <UINT16>

Mode

User Authentication

Description

Set age out inactive users time (minutes).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

age-out 60

Syntax

web-login-session-limit <UINT16>

Mode

User Authentication

Description

Set the maximum login session time for web users.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

web-login-session-limit 60

Syntax

no web-login-session-limit

Mode

User Authentication

Description

Set unlimited login session time for web users.

Example

no web-login-session-limit

Syntax

show-user-status-window

Mode

User Authentication

Description

Enable showing the login status window after web login.

Example

```
show-user-status-window
```

Syntax

```
no show-user-status-window
```

Mode

User Authentication

Description

Disable showing the login status window after web login.

Example

```
no show-user-status-window
```

Syntax

```
status-window-heartbeat { period <TEN_SEC_GRANULARITY_PERIOD> | timeout <UINT16> }
```

Mode

User Authentication

Description

Configure heartbeats sent from the user login status window.

Options

<i>period</i>	Period in seconds.
<i><TEN_SEC_GRANULARITY_PERIOD></i>	A number of seconds that must be a multiple of 10. Example: <i>20</i>
<i>timeout</i>	Time in minutes.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
status-window-heartbeat period 60
```

Syntax

```
disconnected-user-detect
```

Mode

User Authentication

Description

Enable using the login status window heartbeat mechanism for detecting disconnected web users.

Example

```
disconnected-user-detect
```

Syntax

```
no disconnected-user-detect
```

Mode

User Authentication

Description

Disable using the login status window heartbeat mechanism for detecting disconnected web users.

Example

```
no disconnected-user-detect
```

Syntax

```
open-in-same-window
```

Mode

User Authentication

Description

Enable open user's login status window in the same window rather than in a popup.

Example

```
open-in-same-window
```

Syntax

```
no open-in-same-window
```

Mode

User Authentication

Description

Disable open user's login status window in the same window rather than in a popup.

Example

```
no open-in-same-window
```

Syntax

```
rule-auth-bypass-http-url <WORD>
```

Mode

User Authentication

Description

Add a destination URL to be allowed to bypass user authentication in access rules.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
rule-auth-bypass-http-url *.windowsupdate.com...
```

Syntax

```
no rule-auth-bypass-http-url <WORD>
```

Mode

User Authentication

Description

Delete a destination URL to be allowed to bypass user authentication in access rules.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no rule-auth-bypass-http-url *.windowsupdate.com...
```

Syntax

```
acceptable-use-policy
```

Mode

User Authentication

Description

Set the acceptable use policy (AUP) displayed to users during login.

Example

```
acceptable-use-policy
```

Syntax

```
window-size <UINT32> <UINT32>
```

Mode

Acceptable Use Policy

Description

Set the acceptable use policy (AUP) window width and height.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
window-size 460 310
```

Syntax

```
scroll-bars
```

Mode

Acceptable Use Policy

Description

Enable scroll bars on the acceptable use policy (AUP) window.

Example

```
scroll-bars
```

Syntax

```
no scroll-bars
```

Mode

Acceptable Use Policy

Description

Disable scroll bars on the acceptable use policy (AUP) window.

Example

```
no scroll-bars
```

Syntax

```
content <ROL>
```

Mode

Acceptable Use Policy

Description

Set the content for the acceptable use policy (AUP).

Options

<ROL> Remaining command line input.
Example: *line...*

Example

```
content "example template"
```

Syntax

```
no content
```

Mode

Acceptable Use Policy

Description

Clear the content for the acceptable use policy (AUP).

Example

```
no content
```

Syntax

```
aup-on-zones { public | trusted | vpn | wan | wireless }
```

Mode

Acceptable Use Policy

Description

Enable the acceptable use policy (AUP) on login from zones of a given type.

Options

<i>public</i>	On login from public zones.
<i>trusted</i>	On login from trusted zones.
<i>vpn</i>	On login from the VPN zone.
<i>wan</i>	On login from the WAN zone.
<i>wireless</i>	On login from wireless zones.

Example

```
aup-on-zones trusted
```

Syntax

```
no aup-on-zones { public | trusted | vpn | wan | wireless }
```

Mode

Acceptable Use Policy

Description

Disable the acceptable use policy (AUP) on login from from zones of a given type.

Options

<i>public</i>	On login from public zones.
<i>trusted</i>	On login from trusted zones.
<i>vpn</i>	On login from the VPN zone.
<i>wan</i>	On login from the WAN zone.
<i>wireless</i>	On login from wireless zones.

Example

```
no aup-on-zones trusted
```

Syntax

```
customize-login-page { access-barred | access-down | access-unavailable | authentication | disallowed | full | guest-status |  
lockout | logged-out | message | password-update | preempt | redirect | sso-failure | status } <ROL>
```

Mode

User Authentication

Description

Customize login pages.

Options

<i>access-barred</i>	Customize policy access barred page.
<i>access-down</i>	Customize policy access down page.

<i>access-unavailable</i>	Customize policy access unavailable page.
<i>authentication</i>	Customize login authentication page.
<i>disallowed</i>	Customize login disallowed page.
<i>full</i>	Customize login full page.
<i>guest-status</i>	Customize guest login status page.
<i>lockout</i>	Customize login lockout page.
<i>logged-out</i>	Customize logged out page.
<i>message</i>	Customize user login message page.
<i>password-update</i>	Customize user password update page.
<i>preempt</i>	Customize admin preempt page.
<i>redirect</i>	Customize policy login redirect page.
<i>sso-failure</i>	Customize policy SSO probe failure page.
<i>status</i>	Customize login status page.
<ROL>	Remaining command line input. Example: <i>line...</i>

Example

customize-login-page preempt "Preempt page"

Syntax

no customize-login-page { access-barred | access-down | access-unavailable | authentication | disallowed | full | guest-status | lockout | logged-out | message | password-update | preempt | redirect | sso-failure | status }

Mode

User Authentication

Description

Clear specified customized login page.

Options

<i>access-barred</i>	Customize policy access barred page.
<i>access-down</i>	Customize policy access down page.
<i>access-unavailable</i>	Customize policy access unavailable page.
<i>authentication</i>	Customize login authentication page.
<i>disallowed</i>	Customize login disallowed page.
<i>full</i>	Customize login full page.
<i>guest-status</i>	Customize guest login status page.
<i>lockout</i>	Customize login lockout page.
<i>logged-out</i>	Customize logged out page.
<i>message</i>	Customize user login message page.

<i>password-update</i>	Customize user password update page.
<i>preempt</i>	Customize admin preempt page.
<i>redirect</i>	Customize policy login redirect page.
<i>sso-failure</i>	Customize policy SSO probe failure page.
<i>status</i>	Customize login status page.

Example

```
no customize-login-page preempt
```

Syntax

```
track-traffic <IPv4_HOST>
```

Mode

User Authentication

Description

Tracking the traffic.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
track-traffic 2.2.2.2
```

Syntax

```
user local
```

Mode

Config

Description

Configure settings related to local users.

Example

```
user local
```

Syntax

```
apply-password-constraints
```

Mode

Local Users

Description

Enable apply password constraints (configured in `administration_mode`) to all local users (including administrative users, but not the built-in admin account). Note that this command is an alternative to the `administration_mode` command: `constraints-apply-to full-admins limited-admins local-users`.

Example

```
apply-password-constraints
```

Syntax

no apply-password-constraints

Mode

Local Users

Description

Disable apply password constraints (configured in `administration_mode`) for local users.

Example

no apply-password-constraints

Syntax

prune-on-expiry

Mode

Local Users

Description

Enable prune expired local user accounts if a limited lifetime is set.

Example

prune-on-expiry

Syntax

no prune-on-expiry

Mode

Local Users

Description

Disable prune expired local user accounts.

Example

no prune-on-expiry

Syntax

inactivity-timeout <UINT32>

Mode

Local Users

Description

Set a inactivity timeout for all user accounts.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
inactivity-timeout 10
```

Syntax

```
no inactivity-timeout
```

Mode

Local Users

Description

Set a inactivity timeout for all user accounts.

Example

```
inactivity-timeout 10
```

Syntax

```
prune-on-inactive
```

Mode

Local Users

Description

Enable prune inact local user accounts if a inactive timeout is set.

Example

```
prune-on-inactive
```

Syntax

```
no prune-on-inactive
```

Mode

Local Users

Description

Disable prune inactive local user accounts.

Example

```
no prune-on-inactive
```

Syntax

```
domain-name-display-format { automatic | domain-backslash-name | name-at-domain | name-dot-domain }
```

Mode

Local Users

Description

Set display format for domain user/group names.

Options

<i>automatic</i>	Set display format for domain user/group names : Auto-select (from the LDAP server schema)

<i>domain-backslash-name</i>	Set display format for domain user/group names : domain\name
<i>name-at-domain</i>	Set display format for domain user/group names : name@domain.com
<i>name-dot-domain</i>	Set display format for domain user/group names : name.domain

Example

domain_name_display_format automatic

Syntax

user [uuid] <LOCAL_USER_USER_NAME> [domain <LOCAL_USER_DOMAIN_NAME>] [password <ENC_PASSWORD>] [member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME>]

Mode

Local Users

Description

Add or update a local user account.

Options

<i>uuid</i>	Edit a user object by UUID.
<i><LOCAL_USER_USER_NAME></i>	User object name. Example: <i>John</i>
<i>domain</i>	Set the user's domain.
<i><LOCAL_USER_DOMAIN_NAME></i>	User object domain name. Example: <i>example.com</i>
<i>password</i>	Set the user password.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>
<i>member-of</i>	Add membership to a user group for this user.
<i><LOCAL_USER_MEMBER_OF_GROUP_NAME></i>	User group object name. Example: <i>Limited Administrators</i>

Example

user johndoe
user johndoe domain example.com

Syntax

no user [uuid] <LOCAL_USER_USER_NAME> [domain <LOCAL_USER_DOMAIN_NAME>]

Mode

Local Users

Description

Delete a local user account.

Options

<i>uuid</i>	Delete a user object by UUID.
<i><LOCAL_USER_USER_NAME></i>	User object name. Example: <i>John</i>
<i>domain</i>	Set the user's domain.
<i><LOCAL_USER_DOMAIN_NAME></i>	User object domain name. Example: <i>example.com</i>

Example

no user johndoe
no user johndoe domain example.com

Syntax

no users

Mode

Local Users

Description

Delete all local user accounts.

Example

no users

Syntax

group [uuid] <LOCAL_GROUP_GROUP_NAME> [domain <LOCAL_GROUP_DOMAIN_NAME>]

Mode

Local Users

Description

Add or update a local user group.

Options

<i>uuid</i>	Edit a user group object by UUID.
<i><LOCAL_GROUP_GROUP_NAME></i>	User group object name. Example: <i>Limited Administrators</i>
<i>domain</i>	Set the user group's domain.
<i><LOCAL_GROUP_DOMAIN_NAME></i>	User group object domain name. Example: <i>example.com</i>

Example

group "Special Users"
group salesTeam domain example.com

Syntax

no group [uuid] <LOCAL_GROUP_GROUP_NAME> [domain <LOCAL_GROUP_DOMAIN_NAME>]

Mode

Local Users

Description

Delete a local user group.

Options

<i>uuid</i>	Delete a user group object by UUID.
<i><LOCAL_GROUP_GROUP_NAME></i>	User group object name. Example: <i>Limited Administrators</i>
<i>domain</i>	Set the user group's domain.
<i><LOCAL_GROUP_DOMAIN_NAME></i>	User group object domain name. Example: <i>example.com</i>

Example

no group "Special Users"
no group salesTeam domain example.com

Syntax

no groups

Mode

Local Users

Description

Delete all local user groups.

Example

no groups

Syntax

name <LOCAL_USER_USER_NAME>

Mode

Local User

Description

Set the login name of the user account.

Options

<LOCAL_USER_USER_NAME> User object name.
Example: *John*

Example

name johndoe

Syntax

uuid <UUID>

Mode

Local User

Description

Set user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0500-c0eae49ce84c

Syntax

no uuid <UUID>

Mode

Local User

Description

Clear user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

no uuid

Syntax

domain **<LOCAL_USER_DOMAIN_NAME>**

Mode

Local User

Description

Set the user's domain, this is for domain user.

Options

<LOCAL_USER_DOMAIN_NAME> User object domain name.
Example: *example.com*

Example

domain example.com

Syntax

no domain

Mode

Local User

Description

Clear the user's domain, this is for non-domain user.

Example

no domain

Syntax

comment **<WORD>**

Mode

Local User

Description

Set a comment for the user account.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Added 7/26/2010"

Syntax

no comment

Mode

Local User

Description

Clear the comment for the user account.

Example

no comment

Syntax

password <ENC_PASSWORD>

Mode

Local User

Description

Set the user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password pwd1234

Syntax

no password

Mode

Local User

Description

Clear user password.

Syntax

force-password-change

Mode

Local User

Description

Force the user to change the password at the next login.

Example

force-password-change

Syntax

no force-password-change

Mode

Local User

Description

Disable make the user change the password at next login.

Example

no force-password-change

Syntax

expiration <DATE_YYYYMMDD> <TIME_HHMM>

Mode

Local User

Description

Set user's expiration time (absolute time).

Options

<DATE_YYYYMMDD>	Date in the form: YYYY:MM:DD. Example: <i>2010:06:30</i>
<TIME_HHMM>	Time in the form: DD:DD. Example: <i>12:00</i>

Example

expiration 2013:12:31 23:59

Syntax

account-lifetime { days <UINT16> | expired | hours <UINT16> | minutes <UINT16> }

Mode

Local User

Description

Set a limited lifetime for the user account.

Options

days	Set the lifetime in days.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
expired	Expired user.
hours	Set the lifetime in hours.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
minutes	Set the lifetime in minutes.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

account-lifetime minutes 48

Syntax

no account-lifetime

Mode

Local User

Description

Disable the user account to expire.

Example

no account-lifetime

Syntax

prune-on-expiry

Mode

Local User

Description

Delete the user account when it expires if a limited lifetime is set.

Example

prune-on-expiry

Syntax

no prune-on-expiry

Mode

Local User

Description

Disable prune account on expiration.

Example

no prune-on-expiry

Syntax

one-time-password { otp | totp }

Mode

Local User

Description

Set one-time passwords method.

Options

otp OTP via mail.

totp TOTP

Example

```
one-time-password otp
one-time-password totp
```

Syntax

```
no one-time-password
```

Mode

Local User

Description

Disable one-time password required for the user.

Example

```
no one-time-password
```

Syntax

```
unbind-totp-key
```

Mode

Local User

Description

Unbind totp key.

Example

```
unbind-totp-key
```

Syntax

```
email-address <EMAIL>
```

Mode

Local User

Description

Set the user's e-mail address.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
email-address me@myplace.org
```

Syntax

```
no email-address
```

Mode

Local User

Description

Clear the user's e-mail address.

Example

no email-address

Syntax

vpn-client-access { { [ipv4 | ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Local User

Description

Add a local network to which the user will be given access when connecting via VPN client.

Options

ipv4	IPv4 address object.
ipv6	IPv6 address object.
host <ADDR_HOST>	Give VPN client access to an IP address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Give VPN client access to a network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Give VPN client access to an IP address range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Select an existing address group by name. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Select an existing address object by name. Address object name. Example: <i>Web Server</i>

Example

vpn-client-access name "LAN Subnets"

Syntax

no vpn-client-access { group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Local User

Description

Remove a local network from those to which the user gets access when connecting via VPN client.

Options

<i>group</i>	Group address object name.
<i><ADDR_GROUP_NAME_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>name</i>	Address object name.
<i><ADDR_NAME_MIXED></i>	Address object name. Example: <i>Web Server</i>

Example

```
no vpn-client-access name "LAN Subnets"
```

Syntax

```
guest-login-uniqueness
```

Mode

Local User

Description

Enable enforcing a unique guest services login session.

Example

```
guest-login-uniqueness
```

Syntax

```
no guest-login-uniqueness
```

Mode

Local User

Description

Disable enforcing a unique guest services login session.

Example

```
no guest-login-uniqueness
```

Syntax

```
guest-idle-timeout { days <UINT32> | hours <UINT32> | minutes <UINT32> }
```

Mode

Local User

Description

Set the idle timeout for guest services.

Options

<i>days</i>	Set the idle timeout in days.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

- hours** Set the idle timeout in hours.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*
- minutes** Set the idle timeout in minutes.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
guest-idle-timeout minutes 20
```

Syntax

```
no guest-idle-timeout
```

Mode

Local User

Description

Clear the idle timeout for guest services.

Example

```
no guest-idle-timeout
```

Syntax

```
no quota-cycle
```

Mode

Local User

Description

Set no quota cycle for the user.

Example

```
no quota-cycle
```

Syntax

```
quota-cycle { day | month | week }
```

Mode

Local User

Description

Set a quota cycle for the user.

Options

- day** Set the quota cycle as one day.
- month** Set the quota cycle as one month.
- week** Set the quota cycle as one week.

Example

quota-cycle per day

Syntax

```
session-lifetime { days <UINT16> | hours <UINT16> | minutes <UINT16> }
```

Mode

Local User

Description

Set a session time limit for the user.

Options

days Set the session limit in days.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

hours Set the session limit in hours.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

minutes Set the session limit in minutes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
session-lifetime minutes 48
```

Syntax

```
no session-lifetime
```

Mode

Local User

Description

Disable session time limit for the user.

Example

```
no session-lifetime
```

Syntax

```
limit { receive <UINT32> | transmit <UINT32> }
```

Mode

Local User

Description

Set the receive or transmit limit in MB for the user.

Options

receive Set the receive limit in MB for the user.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

transmit Set the transmit limit in MB for the user.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
limit receive 500
limit transmit 300
```

Syntax

```
no limit { receive | transmit }
```

Mode

Local User

Description

Disable receive or transmit limit for the user.

Options

receive Disable receive limit for the user.

transmit Disable transmit limit for the user.

Example

```
no limit receive
no limit transmit
```

Syntax

```
member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME>
```

Mode

Local User

Description

Add membership to a user group for this user.

Options

<LOCAL_USER_MEMBER_OF_GROUP_NAME> User group object name.
Example: Limited Administrators

Example

```
member-of "SonicWALL Administrators"
```

Syntax

```
no member-of <LOCAL_USER_MEMBER_OF_GROUP_NAME>
```

Mode

Local User

Description

Remove a user group membership for this user.

Options

<LOCAL_USER_MEMBER_OF_GROUP_NAME> User group object name.

Example

```
no member-of "SonicWALL Administrators"
```

Syntax

```
no members-of
```

Mode

Local User

Description

Remove all user group membership for this user.

Example

```
no members-of
```

Syntax

```
name <LOCAL_GROUP_GROUP_NAME>
```

Mode

Local Group

Description

Set the name of the user group.

Options

<LOCAL_GROUP_GROUP_NAME>	User group object name. Example: <i>Limited Administrators</i>

Example

```
name "Special Users"
```

Syntax

```
domain <LOCAL_GROUP_DOMAIN_NAME>
```

Mode

Local Group

Description

Set the user group's domain, this is for domain user group.

Options

<LOCAL_GROUP_DOMAIN_NAME>	User group object domain name. Example: <i>example.com</i>

Example

```
domain example.com
```

Syntax

no domain

Mode

Local Group

Description

Clear the user group's domain, this is for non-domain user group.

Example

no domain

Syntax

comment <WORD>

Mode

Local Group

Description

Set a comment for the user group.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Added 7/26/2010"

Syntax

no comment

Mode

Local Group

Description

Remove the comment for the user group.

Example

no comment

Syntax

ldap-location <WORD>

Mode

Local Group

Description

If memberships set by user's location in the LDAP directory is checked, this gives the location in the LDAP directory tree for that.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ldap-location domain.com/users
```

Syntax

```
no ldap-location
```

Mode

Local Group

Description

Clear location in LDAP directory tree for the memberships that are set by user's location in the LDAP directory.

Example

```
no ldap-location
```

Syntax

```
memberships-by-ldap-location { at | under-or-at }
```

Mode

Local Group

Description

Enable memberships are set by user's location in the LDAP directory. For users, they can set the location at or under the given location which you can set by ldap-location command.

Options

at Set the location at the given LDAP location for users.

under-or-at Set the location under or at the given LDAP location for users.

Example

```
memberships-by-ldap-location at
memberships-by-ldap-location under-or-at
```

Syntax

```
no memberships-by-ldap-location
```

Mode

Local Group

Description

Disable memberships are set by user's location in the LDAP directory.

Example

```
no memberships-by-ldap-location
```

Syntax

```
refresh-from-ldap-server
```

Mode

Local Users

Description

Refresh from LDAP server.

Example

```
refresh-from-ldap-server
```

Syntax

```
one-time-password { otp | totp }
```

Mode

Local Group

Description

Set one-time passwords method.

Options

otp OTP via mail.

totp TOTP

Example

```
one-time-password otp
one-time-password totp
```

Syntax

```
no one-time-password
```

Mode

Local Group

Description

Disable one-time password required for the user.

Example

```
no one-time-password
```

Syntax

```
to-management-on-login
```

Mode

Local Group

Description

Members of the group with administrative privilege will go straight to the management UI on web login (only applies for user groups that give administrative privilege).

Example

```
to-management-on-login
```

Syntax

no to-management-on-login

Mode

Local Group

Description

Disable members of the group go straight to the management UI on web login (only applies for user groups that give administrative privilege).

Example

no to-management-on-login

Syntax

read-only-restriction

Mode

Local Group

Description

The administrative rights from the other groups will be restricted to read-only.

Example

read-only-restriction

Syntax

no read-only-restriction

Mode

Local Group

Description

The administrative rights from the other groups override this (no read-only restriction).

Example

no read-only-restriction

Syntax

vpn-client-access { { [ipv4 | ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Local Group

Description

Add a local network to which members of the group will be given access when connecting via VPN client.

Options

<i>ipv4</i>	IPv4 address object.
<i>ipv6</i>	IPv6 address object.
<i>host</i> <i><ADDR_HOST></i>	Give VPN client access to an IP address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network	Give VPN client access to a network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Give VPN client access to an IP address range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Select an existing address group by name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Select an existing address object by name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

vpn-client-access name "LAN Subnets"

Syntax

no vpn-client-access { group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Local Group

Description

Remove a local network from those to which members of the group get access when connecting via VPN client.

Options

group	Group address object name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

no vpn-client-access name "LAN Subnets"

Syntax

member <LOCAL_USER_AND_GROUP_NAME>

Mode

Local Group

Description

Add membership to this group for the named user or user group.

Options

<LOCAL_USER_AND_GROUP_NAME> Local user and user group object display name.
Example: *Limited Administrators*

Example

member "All LDAP Users"

Syntax

no member <LOCAL_USER_AND_GROUP_NAME>

Mode

Local Group

Description

Remove a member from the group.

Options

<LOCAL_USER_AND_GROUP_NAME> Local user and user group object display name.
Example: *Limited Administrators*

Example

no member "All LDAP Users"

Syntax

no members

Mode

Local Group

Description

Remove all member from the group.

Example

no members

Syntax

uuid <UUID>

Mode

Local Group

Description

Set user group object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0600-c0eae49ce84c

Syntax

no uuid <UUID>

Mode

Local Group

Description

Clear user group object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

no uuid

Syntax

bookmark <SSLVPN_BOOKMARK>

Mode

Local User

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

bookmark "Admin Desktop"

Syntax

no bookmark <SSLVPN_BOOKMARK>

Mode

Local User

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no bookmark "Admin Work Desktop"

Syntax

no bookmarks

Mode

Local User

Description

Delete all bookmarks.

Example

```
no bookmarks
```

Syntax

```
name <SSLVPN_BOOKMARK>
```

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Admin Work Desktop"
```

Syntax

```
host <WORD>
```

Mode

Bookmark

Description

Set host name or IP address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
host 192.168.168.57
```

Syntax

```
no host
```

Mode

Bookmark

Description

Clear host name or IP address.

Example

```
no host
```

Syntax

```
service { rdp | sshv2 | telnet | vnc }
```

Mode

Bookmark

Description

Set bookmark service type.

Options

rdp Terminal services (RDP-HTML5).

sshv2 Secure shell version 2 (SSHv2).

telnet Telnet.

vnc Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

RDP

Description

Set screen size.

Options

1024x768 1024x768.

1280x1024 1280x1024.

640x480 640x480.

800x600 800x600.

full-screen Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

RDP

Description

Set screen colors.

Options

- 15bit** 15 bit - high color.
- 16bit** 16 bit - high color.
- 24bit** 24 bit - high color.
- 256** 256 bit.
- 32bit** 32 bit - highest quality.

Example

colors 24bit

Syntax

application-path <WORD>

Mode

RDP

Description

Set application and path to launch.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

application-path "C:\\\\Remote Applications\\\\myapp.exe"

Syntax

no application-path

Mode

RDP

Description

Clear application and path.

Example

no application-path

Syntax

start-in-folder <WORD>

Mode

RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

start-in-folder "C:\\Work\\"

Syntax

no start-in-folder

Mode

RDP

Description

Clear folder to start in.

Example

no start-in-folder

Syntax

automatic-login { custom [name <WORD>] [password <ENC_PASSWORD>] [domain <WORD>] | ssl-vpn }

Mode

RDP

Description

Enable automatically log in.

Options

<i>custom</i>	Use custom account credentials.
<i>name</i>	Enter login name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>password</i>	Enter login password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>
<i>domain</i>	Enter login domain.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>ssl-vpn</i>	Use SSL-VPN account credentials.

Example

automatic-login custom name myuser password mypassword domain mydomain

Syntax

no automatic-login [custom { domain | name | password }]

Mode

RDP

Description

Disable automatically log in.

Options

<i>custom</i>	Use custom account credentials.
<i>domain</i>	Clear login domain.
<i>name</i>	Clear login name.
<i>password</i>	Clear login password.

Example

```
no automatic-login
no automatic-login custom name
no automatic-login custom password
no automatic-login custom domain
```

Syntax

```
redirect-clipboard
```

Mode

RDP

Description

Enable redirect clipboard.

Example

```
redirect-clipboard
```

Syntax

```
no redirect-clipboard
```

Mode

RDP

Description

Disable redirect clipboard.

Example

```
no redirect-clipboard
```

Syntax

```
redirect-audio
```

Mode

RDP

Description

Enable redirect audio.

Example

```
redirect-audio
```

Syntax

no redirect-audio

Mode

RDP

Description

Disable redirect audio.

Example

no redirect-audio

Syntax

auto-reconnection

Mode

RDP

Description

Enable automatic reconnection.

Example

auto-reconnection

Syntax

no auto-reconnection

Mode

RDP

Description

Disable automatic reconnections.

Example

no auto-reconnection

Syntax

desktop-background

Mode

RDP

Description

Enable desktop background.

Example

desktop-background

Syntax

no desktop-background

Mode

RDP

Description

Disable desktop background.

Example

no desktop-background

Syntax

window-drag

Mode

RDP

Description

Enable window drag.

Example

window-drag

Syntax

no window-drag

Mode

RDP

Description

Disable window drag.

Example

no window-drag

Syntax

animation

Mode

RDP

Description

Enable menu / window animation.

Example

animation

Syntax

no animation

Mode

RDP

Description

Disable menu / window animation.

Example

```
no animation
```

Syntax

```
view-only
```

Mode

VNC

Description

Enable view only.

Example

```
view-only
```

Syntax

```
no view-only
```

Mode

VNC

Description

Disable view only.

Example

```
no view-only
```

Syntax

```
share-desktop
```

Mode

VNC

Description

Enable share desktop.

Example

```
share-desktop
```

Syntax

```
no share-desktop
```

Mode

VNC

Description

Disable share desktop.

Example

```
no share-desktop
```

Syntax

```
automatic-accept-host-key
```

Mode

SSHV2

Description

Enable automatically accept host key.

Example

```
automatic-accept-host-key
```

Syntax

```
no automatic-accept-host-key
```

Mode

SSHV2

Description

Disable automatically accept host key.

Example

```
no automatic-accept-host-key
```

Syntax

```
display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

```
display-on-mobile
```

Syntax

```
no display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

```
no display-on-mobile
```

Syntax

```
bookmark <SSLVPN_BOOKMARK>
```

Mode

Local Group

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
bookmark "Admin Desktop"
```

Syntax

```
no bookmark <SSLVPN_BOOKMARK>
```

Mode

Local Group

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no bookmark "Admin Work Desktop"
```

Syntax

```
no bookmarks
```

Mode

Local Group

Description

Delete all bookmarks.

Example

```
no bookmarks
```

Syntax

```
name <SSLVPN_BOOKMARK>
```

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Admin Work Desktop"
```

Syntax

```
host <WORD>
```

Mode

Bookmark

Description

Set host name or IP address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
host 192.168.168.57
```

Syntax

```
no host
```

Mode

Bookmark

Description

Clear host name or IP address.

Example

```
no host
```

Syntax

```
service { rdp | sshv2 | telnet | vnc }
```

Mode

Bookmark

Description

Set bookmark service type.

Options

<i>rdp</i>	Terminal services (RDP-HTML5).
<i>sshv2</i>	Secure shell version 2 (SSHv2).
<i>telnet</i>	Telnet.
<i>vnc</i>	Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

RDP

Description

Set screen size.

Options

<i>1024x768</i>	1024x768.
<i>1280x1024</i>	1280x1024.
<i>640x480</i>	640x480.
<i>800x600</i>	800x600.
<i>full-screen</i>	Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

RDP

Description

Set screen colors.

Options

<i>15bit</i>	15 bit - high color.
<i>16bit</i>	16 bit - high color.
<i>24bit</i>	24 bit - high color.
<i>256</i>	256 bit.
<i>32bit</i>	32 bit - highest quality.

Example

```
colors 24bit
```

Syntax

```
application-path <WORD>
```

Mode

RDP

Description

Set application and path to launch.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
application-path "C:\\\\Remote Applications\\\\myapp.exe"
```

Syntax

```
no application-path
```

Mode

RDP

Description

Clear application and path.

Example

```
no application-path
```

Syntax

```
start-in-folder <WORD>
```

Mode

RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
start-in-folder "C:\\Work\\"
```

Syntax

```
no start-in-folder
```


Mode

RDP

Description

Clear folder to start in.

Example

```
no start-in-folder
```

Syntax

```
automatic-login { custom [ name <WORD> ] [ password <ENC_PASSWORD> ] [ domain <WORD> ] | ssl-vpn }
```

Mode

RDP

Description

Enable automatically log in.

Options

custom	Use custom account credentials.
name	Enter login name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
password	Enter login password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>
domain	Enter login domain.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
ssl-vpn	Use SSL-VPN account credentials.

Example

```
automatic-login custom name myuser password mypassword domain mydomain
```

Syntax

```
no automatic-login [ custom { domain | name | password } ]
```

Mode

RDP

Description

Disable automatically log in.

Options

custom	Use custom account credentials.
domain	Clear login domain.
name	Clear login name.
password	Clear login password.

Example

```
no automatic-login  
no automatic-login custom name
```

```
no automatic-login custom password
no automatic-login custom domain
```

Syntax

```
redirect-clipboard
```

Mode

RDP

Description

Enable redirect clipboard.

Example

```
redirect-clipboard
```

Syntax

```
no redirect-clipboard
```

Mode

RDP

Description

Disable redirect clipboard.

Example

```
no redirect-clipboard
```

Syntax

```
redirect-audio
```

Mode

RDP

Description

Enable redirect audio.

Example

```
redirect-audio
```

Syntax

```
no redirect-audio
```

Mode

RDP

Description

Disable redirect audio.

Example

```
no redirect-audio
```

Syntax

auto-reconnection

Mode

RDP

Description

Enable automatic reconnection.

Example

auto-reconnection

Syntax

no auto-reconnection

Mode

RDP

Description

Disable automatic reconnections.

Example

no auto-reconnection

Syntax

desktop-background

Mode

RDP

Description

Enable desktop background.

Example

desktop-background

Syntax

no desktop-background

Mode

RDP

Description

Disable desktop background.

Example

no desktop-background

Syntax

window-drag

Mode

RDP

Description

Enable window drag.

Example

window-drag

Syntax

no window-drag

Mode

RDP

Description

Disable window drag.

Example

no window-drag

Syntax

animation

Mode

RDP

Description

Enable menu / window animation.

Example

animation

Syntax

no animation

Mode

RDP

Description

Disable menu / window animation.

Example

no animation

Syntax

view-only

Mode

VNC

Description

Enable view only.

Example

view-only

Syntax

no view-only

Mode

VNC

Description

Disable view only.

Example

no view-only

Syntax

share-desktop

Mode

VNC

Description

Enable share desktop.

Example

share-desktop

Syntax

no share-desktop

Mode

VNC

Description

Disable share desktop.

Example

no share-desktop

Syntax

automatic-accept-host-key

Mode

SSHV2

Description

Enable automatically accept host key.

Example

```
automatic-accept-host-key
```

Syntax

```
no automatic-accept-host-key
```

Mode

SSHV2

Description

Disable automatically accept host key.

Example

```
no automatic-accept-host-key
```

Syntax

```
display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

```
display-on-mobile
```

Syntax

```
no display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

```
no display-on-mobile
```

Syntax

```
unbind-totp-key <LOCAL_USER_USER_NAME>
```

Mode

Local Users

Description

Unbind totp key.

Options

<LOCAL_USER_USER_NAME> User object name.
Example: *John*

Example

unbind-totp-key

Syntax

kill-user name <USER_LOGIN_NAME>

Mode

Top Level
User Management
Config

Description

Log out users.

Options

<USER_LOGIN_NAME> A connected user's login name.
Example: *jdoe*

Example

kill-user name guest1

Syntax

kill-user at <USER_MIXED_ADDR> [user <UINT32>]

Mode

Top Level
User Management
Config

Description

Log out users.

Options

<USER_MIXED_ADDR> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*
user For Terminal Services users only, selects the user at the IP address.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

kill-user at 192.168.168.1

Syntax

kill-user inactive at <USER_MIXED_ADDR>

Mode

Description

Log out inactive users.

Options

<USER_MIXED_ADDR> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Example

kill-user inactive at 192.168.168.1

Syntax

unlock-ip <USER_MIXED_ADDR>

Mode

Description

Unlock an IP address that has been locked out due to too many failed login attempts.

Options

<USER_MIXED_ADDR> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Example

unlock-ip 192.168.168.1

Syntax

unlock-account <WORD>

Mode

Description

Unlock an local account that has been locked out due to too many failed login attempts.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

unlock-account usera

Syntax

user management

Mode

Description

User management.

Example

```
user management
```

Syntax

```
include { inactive-users | unauthenticated-users }
```

Mode

User Management

Description

Enable show inactive or unauthenticated users' status.

Options

inactive-users Enable show inactive users' status.

unauthenticated-users Enable show unauthenticated users' status.

Example

```
include inactive-users
include unauthenticated-users
```

Syntax

```
no include { inactive-users | unauthenticated-users }
```

Mode

User Management

Description

Disable show inactive or unauthenticated users' status.

Options

inactive-users Disable show inactive users' status.

unauthenticated-users Disable show unauthenticated users' status.

Example

```
no include inactive-users
no include unauthenticated-users
```

Syntax

```
send-message message <WORD> ip-address <IPV4_HOST>
```

Mode

Top Level
Config

Description

send message to the user.

Options

<i>message</i>	Message to send.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>ip-address</i>	ip-address of the user.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
send-message message hello ip-address 10.65.131.78
```

Syntax

```
user radius
```

Mode

Config

Description

Configure RADIUS settings.

Example

```
user radius
```

Syntax

```
clear user radius statistics [ server <RADIUS_SERVER_HOST_NAME> ]
```

Mode

RADIUS
Top Level
Config

Description

Reset RADIUS statistics.

Options

<i>server</i>	Reset a specific RADIUS server statistics.
<i><RADIUS_SERVER_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>

Example

```
clear user radius statistics  
clear user radius statistics server 10.10.10.10
```

Syntax

```
local-users-only
```

Mode

RADIUS

Description

Limit login to only RADIUS users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

no local-users-only

Mode

RADIUS

Description

Don't limit login to only RADIUS users with accounts in the local user database.

Example

no local-users-only

Syntax

default-user-group <LOCAL_USER_GROUP_NAME>

Mode

RADIUS

Description

Select a user group to whom all users who are authenticated via RADIUS will be given membership by default (i.e. a group that can be used to set accesses etc. that will apply to all RADIUS users).

Options

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

default-user-group "Radius Users"

Syntax

no default-user-group

Mode

RADIUS

Description

RADIUS will not be given membership to any user group by default.

Example

no default-user-group

Syntax

timeout <UINT32>

Mode

RADIUS

Description

Set the timeout for the RADIUS servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
timeout 10
```

Syntax

```
retries <UINT32>
```

Mode

RADIUS

Description

Set the number of retries for the RADIUS servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
retries 10
```

Syntax

```
periodic-check-server
```

Mode

RADIUS

Description

Enable periodically check RADIUS servers that are down.

Example

```
periodic-check-server
```

Syntax

```
no periodic-check-server
```

Mode

RADIUS

Description

Disable periodically check RADIUS servers that are down.

Example

```
no periodic-check-server
```

Syntax

```
mschapv2-mode
```

Mode

RADIUS

Description

Enfore MSCHAPv2 mode.

Example

```
mschapv2-mode
```

Syntax

```
no mschapv2-mode
```

Mode

RADIUS

Description

Do no enfore MSCHAPv2 mode.

Example

```
no mschapv2-mode
```

Syntax

```
user-group-mechanism { ldap | local-only | radius-attribute { filter-id | vendor-specific } }
```

Mode

RADIUS

Description

Set the mechanism to use to set user group memberships for users who are authenticated via RADIUS.

Options

<i>ldap</i>	Read user groups via LDAP.
<i>local-only</i>	Set using local users that duplicate RADIUS users.
<i>radius-attribute</i>	Read user groups via a RADIUS attribute.
<i>filter-id</i>	Use the standard RADIUS filter-id attribute.
<i>vendor-specific</i>	Use the SonicWall vendor-specific RADIUS attribute.

Example

```
user-group-mechanism radius-attribute filter-id
```

Syntax

```
server <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS

Description

Configure a RADIUS server.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

```
server 192.168.168.16
```

Syntax

```
no server <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS

Description

Delete a RADIUS server.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

```
no server 192.168.168.16
```

Syntax

```
no servers
```

Mode

RADIUS

Description

Delete all RADIUS servers.

Example

```
no servers
```

Syntax

```
enable
```

Mode

RADIUS Server

Description

Enable the RADIUS server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

RADIUS Server

Description

Disable the RADIUS server.

Example

```
no enable
```

Syntax

```
host <RADIUS_SERVER_HOST_NAME>
```

Mode

RADIUS Server

Description

Set the RADIUS server's host name or IP address.

Options

<RADIUS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\nwww.radiusServer.com*

Example

```
host 192.168.168.1
```

Syntax

```
port <IPV4_PORT>
```

Mode

RADIUS Server

Description

Set the RADIUS server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 1812
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

RADIUS Server

Description

Set the RADIUS server's shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret mysecret
```

Syntax

```
no shared-secret
```

Mode

RADIUS Server

Description

Clear the RADIUS server's shared secret.

Example

```
no shared-secret
```

Syntax

```
send-through-vpn-tunnel
```

Mode

RADIUS Server

Description

Enable enforce send packet through vpn tunnel.

Example

```
send-through-vpn-tunnel
```

Syntax

```
no send-through-vpn-tunnel
```

Mode

RADIUS Server

Description

Disable enforce send packet through vpn tunnel.

Example

```
no send-through-vpn-tunnel
```

Syntax

```
user-name-format { any | down-level-logon | name-dot-domain | user-name | user-principle }
```

Mode

RADIUS Server

Description

Set user name attribute format.

Options

<i>any</i>	Set to any format.
<i>down-level-logon</i>	Set to \"Domain\\User-name\" format.
<i>name-dot-domain</i>	Set to \"User-name.Domain\" format.
<i>user-name</i>	Set to \"User-name\" format.
<i>user-principle</i>	Set to \"User-name@Domain\" format.

Example

```
user-name-format simple-name
```

Syntax

```
test <RADIUS_SERVER_HOST_NAME> [ user <WORD> <WORD> [ auth-method { chap | mschap | mschapv2 } ] ]
```

Mode

RADIUS

Description

Run the RADIUS test using specified server.

Options

<i><RADIUS_SERVER_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\nwww.radiusServer.com</i>
<i>user</i>	Run the RADIUS user test with the given user name/password.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>auth-method</i>	select a authentication method.
<i>chap</i>	Run the test with RADIUS in CHAP mode.
<i>mschap</i>	Run the test with RADIUS in MSCHAP mode.
<i>mschapv2</i>	Run the test with RADIUS in MSCHAPv2 mode.

Example

```
test 192.168.168.16
test 192.168.168.16 user user1 pwd1234
```

Syntax

```
accounting
```

Mode

RADIUS

Description

Configure RADIUS accounting settings.

Example

```
accounting
```

Syntax

```
server <RADIUS_ACCOUNTING_HOST_NAME>
```

Mode

RADIUS Accounting

Description

Configure a RADIUS accounting server.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: `10.10.10.10\www.radiusServer.com`

Example

```
server 192.168.168.16
```

Syntax

```
no server <RADIUS_ACCOUNTING_HOST_NAME>
```

Mode

RADIUS Accounting

Description

Delete a RADIUS accounting server.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: `10.10.10.10\www.radiusServer.com`

Example

```
no server 192.168.168.16
```

Syntax

```
no servers
```

Mode

RADIUS Accounting

Description

Delete all RADIUS accounting servers.

Example

```
no servers
```

Syntax

```
enable
```

Mode

RADIUS Accounting Server

Description

Enable the RADIUS accounting server.

Example

enable

Syntax

no enable

Mode

RADIUS Accounting Server

Description

Disable the RADIUS accounting server.

Example

no enable

Syntax

host <RADIUS_ACCOUNTING_HOST_NAME>

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's host name or IP address.

Options

<RADIUS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.radiusServer.com*

Example

host 192.168.168.1

Syntax

port <IPV4_PORT>

Mode

RADIUS Accounting Server

Description

Set the RADIUS accounting server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 1812

Syntax

shared-secret <ENC_PASSWORD>

Mode

Description

Set the RADIUS accounting server's shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret mysecret
```

Syntax

```
no shared-secret
```

Mode

RADIUS Accounting Server

Description

Clear the RADIUS accounting server's shared secret.

Example

```
no shared-secret
```

Syntax

```
user-name-format { down-level-logon | name-dot-domain | user-name | user-principle }
```

Mode

RADIUS Accounting Server

Description

Set user name attribute format.

Options

down-level-logon Set to \"Domain\\User-name\" format.

name-dot-domain Set to \"User-name.Domain\" format.

user-name Set to \"User-name\" format.

user-principle Set to \"User-name@Domain\" format.

Example

```
user-name-format user-name
```

Syntax

```
test <RADIUS_ACCOUNTING_HOST_NAME> [ user <WORD> <IPV4_HOST> ]
```

Mode

RADIUS Accounting

Description

Run the RADIUS accounting server test using specified server.

Options

<RADIUS_ACCOUNTING_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>
user	Run the RADIUS user test with the given user name/ip address.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
test 192.168.168.16
test 192.168.168.16 user user1 192.168.168.1
```

Syntax

```
timeout <UINT32>
```

Mode

RADIUS Accounting

Description

Set the timeout for the RADIUS accounting servers.

Options

<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
timeout 10
```

Syntax

```
retries <UINT32>
```

Mode

RADIUS Accounting

Description

Set the number of retries for the RADIUS accounting servers.

Options

<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
retries 10
```

Syntax

```
data { all-servers | guest-users | remote-client-users | sso-authenticated-users | sso-users-identified-via-radius-accounting | users-authenticated-by-web-login }
```

Mode

RADIUS Accounting

Description

Enable sending accounting data to servers or for users.

Options

<i>all-servers</i>	Enable sending accounting data to all servers.
<i>guest-users</i>	Enable sending accounting data for guest users.
<i>remote-client-users</i>	Enable sending accounting data for remote client users.
<i>sso-authenticated-users</i>	Enable sending accounting data for SSO-authenticated users.
<i>sso-users-identified-via-radius-accounting</i>	Enable including SSO users identified via RADIUS Accounting.
<i>users-authenticated-by-web-login</i>	Enable sending accounting data for users authenticated by web login.

Example

```
data all-servers
data users-authenticated-by-web-login
data remote-client-users
data guest-users
data sso-authenticated-users
data sso-users-identified-via-radius-accounting
```

Syntax

```
no data { all-servers | guest-users | remote-client-users | sso-authenticated-users | sso-users-identified-via-radius-accounting | users-authenticated-by-web-login }
```

Mode

RADIUS Accounting

Description

Disable sending accounting data to servers or for users.

Options

<i>all-servers</i>	Enable sending accounting data to all servers.
<i>guest-users</i>	Disable sending accounting data for guest users.
<i>remote-client-users</i>	Disable sending accounting data for remote client users.
<i>sso-authenticated-users</i>	Disable sending accounting data for SSO-authenticated users.
<i>sso-users-identified-via-radius-accounting</i>	Enable including SSO users identified via RADIUS Accounting.
<i>users-authenticated-by-web-login</i>	Disable sending accounting data for users authenticated by web login.

Example

```
no data all-servers
no data users-authenticated-by-web-login
no data remote-client-users
no data guest-users
no data sso-authenticated-users
no sso-users-identified-via-radius-accounting
```

Syntax

```
include { domain-and-local-users | domain-users | local-users }
```

Mode

RADIUS Accounting

Description

Include different users in user accounting.

Options

domain-and-local-users Include local and domain users in user accounting.

domain-users Include domain users in user accounting.

local-users Include local users in user accounting.

Example

```
include domain-users
include local-users
include domain-and-local-users
```

Syntax

```
interim-updates <UINT8>
```

Mode

RADIUS Accounting

Description

Set the send interim updates for user accounting.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interim-updates 15
```

Syntax

```
no interim-updates
```

Mode

RADIUS Accounting

Description

Disable the send interim updates for user accounting.

Example

```
no interim-updates
```

Syntax

```
user ldap
```

Mode

Config

Description

Configure LDAP settings.

Example

user ldap

Syntax

```
clear user ldap statistics [ global | server <LDAP_SERVER_HOST_NAME> ]
```

Mode

LDAP
Top Level
Config

Description

Reset LDAP statistics.

Options

global	Reset LDAP global statistics.
server	Reset a specific LDAP server statistics.
<LDAP_SERVER_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i>

Example

```
clear user ldap statistics
clear user ldap statistics global
clear user ldap statistics server 10.10.10.10
```

Syntax

```
protocol-version <UINT8>
```

Mode

LDAP

Description

Set protocol version of LDAP server.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
protocol-version 3
```

Syntax

```
require-valid-certificate
```

Mode

LDAP

Description

Enable validate the certificate presented by the server during the TLS exchange.

Example

```
require-valid-certificate
```

Syntax

```
no require-valid-certificate
```

Mode

LDAP

Description

Disable validate the certificate presented by the server during the TLS exchange.

Example

```
no require-valid-certificate
```

Syntax

```
local-tls-certificate <CERT_NAME>
```

Mode

LDAP

Description

Select a local certificate to use with LDAP if using TLS. This is not normally required but may be if the LDAP server is configured to require a valid certificate from the client (e.g. on a server that allows reading back passwords from user objects when bound as an administrator).

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

Example

```
local-tls-certificate my_ldap_server
```

Syntax

```
no local-tls-certificate
```

Mode

LDAP

Description

Clear local certificate for TLS.

Example

```
no local-tls-certificate
```

Syntax

```
allow-referrals
```

Mode

LDAP

Description

Allow following referrals to other LDAP servers.

Example

```
allow-referrals
```

Syntax

no allow-referrals

Mode

LDAP

Description

Ignore referrals to other LDAP servers.

Example

no allow-referrals

Syntax

allow-references { auto-configuration | domain-search | other-search | user-authentication }

Mode

LDAP

Description

Allow following continuation references to look for more results on other LDAP servers.

Options

<i>auto-configuration</i>	Follow continuation references during auto-configuration.
<i>domain-search</i>	Follow continuation references when searching for domains.
<i>other-search</i>	Follow continuation references in other searches.
<i>user-authentication</i>	Follow continuation references during user authentication.

Example

allow-references user-authentication
allow-references auto-configuration
allow-references domain-search
allow-references other-search

Syntax

no allow-references { auto-configuration | domain-search | other-search | user-authentication }

Mode

LDAP

Description

Disable follow continuation references to look for more results on other LDAP servers when doing particular operations.

Options

<i>auto-configuration</i>	Disable follow references during auto-configuration.
<i>domain-search</i>	Disable follow references when searching for domains.
<i>other-search</i>	Disable follow references in other searches.
<i>user-authentication</i>	Disable follow references during user authentication.

Example

```
no allow-references auto-configuration
no allow-references user-authentication
no allow-references domain-search
```

Syntax

```
local-users-only
```

Mode

LDAP

Description

Limit login to only LDAP users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

```
no local-users-only
```

Mode

LDAP

Description

Don't limit login to only LDAP users with accounts in the local user database.

Example

```
no local-users-only
```

Syntax

```
default-user-group <LOCAL_USER_GROUP_NAME>
```

Mode

LDAP

Description

Select a user group to whom all users who are authenticated via LDAP will be given membership by default (i.e. a group that can be used to set accesses etc. that will apply to all LDAP users).

Options

<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>

Example

```
default-user-group "LDAP Users"
```

Syntax

```
no default-user-group
```

Mode

LDAP

Description

LDAP will not be given membership to any user group by default.

Example

```
no default-user-group
```

Syntax

```
check-deleted-groups-method { after-every-periodic-checks <UINT32> | disabled | read-from-servers }
```

Mode

LDAP

Description

Select a method to check for deleted user groups with Global Catalog.

Options

after-every-periodic-checks	Do a full import after every nth periodic checks.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
disabled	Don't do anything, user must do it manually.
read-from-servers	Read direct from the individual domain servers.

Example

```
check-deleted-groups-method full-import-after-every-periodic-checks 10
```

Syntax

```
mirror-user-groups [ all | have-members | refresh { now | period <UINT32> } ]
```

Mode

LDAP

Description

Enable/config mirror LDAP user groups locally.

Options

all	Mirror all user groups on the LDAP server.
have-members	Only mirror groups that have member users or groups.
refresh	Refresh mirrored LDAP user groups.
now	Refresh now.
period	Set refresh period.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

```
mirror-user-groups
mirror-user-groups all
mirror-user-groups have-members
```

```
mirror-user-groups refresh period 5
mirror-user-groups refresh now
```

Syntax

```
no mirror-user-groups
```

Mode

LDAP

Description

Disable mirror LDAP user groups locally.

Example

```
no mirror-user-groups
```

Syntax

```
exclude-tree <LDAP_EXCLUDE_TREE>
```

Mode

LDAP

Description

Enable exclude user groups in the specified sub-tree from the mirroring.

Options

<LDAP_EXCLUDE_TREE> LDAP exclude tree.
Example: *abc*

Example

```
exclude-tree mydomain.com/groups
```

Syntax

```
no exclude-tree <LDAP_EXCLUDE_TREE>
```

Mode

LDAP

Description

Disable exclude user groups in the specified sub-tree from the mirroring.

Options

<LDAP_EXCLUDE_TREE> LDAP exclude tree.
Example: *abc*

Example

```
no exclude-tree mydomain.com/groups
```

Syntax

```
relay
```

Mode

LDAP

Description

Configure the RADIUS to LDAP relay.

Example

```
relay
```

Syntax

```
enable
```

Mode

LDAP Relay

Description

Enable RADIUS to LDAP Relay.

Example

```
enable
```

Syntax

```
no enable
```

Mode

LDAP Relay

Description

Disable RADIUS to LDAP Relay.

Example

```
no enable
```

Syntax

```
clients-connect { public-zones | trusted-zones | vpn-zone | wan-zone | wireless-zones }
```

Mode

LDAP Relay

Description

Enable specified zone to allow incoming RADIUS requests.

Options

<i>public-zones</i>	Allow incoming RADIUS requests from public zones.
<i>trusted-zones</i>	Allow incoming RADIUS requests from trusted zones.
<i>vpn-zone</i>	Allow incoming RADIUS requests from vpn zone.
<i>wan-zone</i>	Allow incoming RADIUS requests from wan zone.
<i>wireless-zones</i>	Allow incoming RADIUS requests from wireless zones.

Example

```
clients-connect-via wan-zone
clients-connect-via trusted-zones
clients-connect-via public-zones
```

Syntax

```
no clients-connect { public-zones | trusted-zones | vpn-zone | wan-zone | wireless-zones }
```

Mode

LDAP Relay

Description

Disable specified zone to discard incoming RADIUS requests.

Options

<i>public-zones</i>	Discard incoming RADIUS requests from public zones.
<i>trusted-zones</i>	Discard incoming RADIUS requests from trusted zones.
<i>vpn-zone</i>	Discard incoming RADIUS requests from vpn zone.
<i>wan-zone</i>	Discard incoming RADIUS requests from wan zone.
<i>wireless-zones</i>	Discard incoming RADIUS requests from wireless zones.

Example

```
no clients-connect-via wan-zone
no clients-connect-via trusted-zones
no clients-connect-via public-zones
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

LDAP Relay

Description

Set RADIUS shared secret.

Options

<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>

Example

```
shared-secret 123abc
```

Syntax

```
no shared-secret
```

Mode

LDAP Relay

Description

Clear RADIUS shared secret.

Example

```
no shared-secret
```

Syntax

```
legacy-user-group { internet <WORD> | l2tp <WORD> | vpn <WORD> | vpn-client <WORD> }
```

Mode

LDAP Relay

Description

Set the user group that corresponds to the legacy access privileges. These settings allow inter-operation with remote SonicWALL running non-enhanced firmware that do not support user groups. When a user in one of the given user groups is authenticated, the remote SonicWALL will be informed that the user is to be given the relevant privilege.

Options

internet	Set the user group for users with Internet access.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
l2tp	Set the user group for L2TP users.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
vpn	Set the user group for VPN users.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
vpn-client	Set the user group for VPN client users.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
legacy-user-group vpn "WAN GroupVPN"  
legacy-user-group vpn-client "VPN Services"  
legacy-user-group l2tp "My l2tp group"  
legacy-user-group internet "My internet"
```

Syntax

```
no legacy-user-group { internet | l2tp | vpn | vpn-client }
```

Mode

LDAP Relay

Description

Clear the user group that corresponds to the legacy access privileges.

Options

internet	Clear the user group for users with Internet access.
l2tp	Clear the user group for L2TP users.
vpn	Clear the user group for VPN users.
vpn-client	Clear the user group for VPN client users.

Example

```
no legacy-user-group vpn  
no legacy-user-group vpn-client
```



```
no legacy-user-group l2tp
no legacy-user-group internet
```

Syntax

```
server <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP

Description

Add/edit an LDAP server.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
server 192.168.168.1
```

Syntax

```
no server <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP

Description

Delete an LDAP server.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
no server 192.168.168.1
```

Syntax

```
no servers
```

Mode

LDAP

Description

Delete all LDAP servers.

Example

```
no servers
```

Syntax

```
save dynamic-secondary <LDAP_DYNAMIC_SERVER_NAME>
```

Mode

LDAP

Description

Make dynamically learned secondary servers configuration permanent.

Options

<LDAP_DYNAMIC_SERVER_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Dynamic-Server*

Example

```
save dynamic-secondary 192.168.168.16
```

Syntax

```
no dynamic-server <LDAP_DYNAMIC_SERVER_NAME>
```

Mode

LDAP

Description

Delete specified dynamic ldap server.

Options

<LDAP_DYNAMIC_SERVER_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Dynamic-Server*

Example

```
no dynamic-server 10.11.102.103
```

Syntax

```
enable
```

Mode

LDAP Server

Description

Enable the LDAP server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

LDAP Server

Description

Disable the LDAP server.

Example

```
no enable
```

Syntax

```
host <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP Server

Description

Set the LDAP server's host name or IP address.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
host 192.168.168.1
```

Syntax

```
role { backup | primary | secondary }
```

Mode

LDAP Server

Description

Set the LDAP server's role.

Options

backup Backup/replica LDAP server.

primary Primary LDAP server.

secondary Secondary LDAP server.

Example

```
role primary
role secondary
role backup
```

Syntax

```
port <IPV4_PORT>
```

Mode

LDAP Server

Description

Set the LDAP server's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 389
```

Syntax

```
timeout { operation <UINT32> | server <UINT32> }
```

Mode

LDAP Server

Description

Set the timeout for LDAP server.
 The server timeout is the maximum time to wait for each response from the LDAP server over the network. The overall operation timeout is the maximum time to spend on an LDAP operation (including auto-configuration operations that can involve large numbers of requests sent to multiple LDAP servers).

Options

operation Set the overall timeout on an LDAP operation.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

server Set the server timeout which is the maximum time to wait for each response from the LDAP server over the network.

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
timeout operation 5
timeout server 10
```

Syntax

```
use-tls
```

Mode

LDAP Server

Description

Enable use transport layer security (TLS) when log in to the LDAP server.

Example

```
use-tls
```

Syntax

```
no use-tls
```

Mode

LDAP Server

Description

Disable use transport layer security (TLS) when log in to the LDAP server.

Example

```
no use-tls
```

Syntax

```
send-start-tls-request
```

Mode

LDAP Server

Description

Enable send LDAP 'Start TLS' request. This is an LDAP feature that allows an LDAP server to operate in both TLS and non-TLS modes on the same TCP port. You only need check this if your LDAP server uses the same port number for both TLS and non-TLS.

Example

```
send-start-tls-request
```

Syntax

```
no send-start-tls-request
```

Mode

LDAP Server

Description

Disable send LDAP 'Start TLS' request.

Example

```
no send-start-tls-request
```

Syntax

```
backup-for <LDAP_SERVER_HOST_NAME>
```

Mode

LDAP Server

Description

Set the LDAP server for which this is the backup for.

Options

<LDAP_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *LDAP-Server*

Example

```
backup-for 192.168.168.15
```

Syntax

```
no backup-for
```

Mode

LDAP Server

Description

Clear the backup LDAP server.

Example

```
no backup-for
```

Syntax

```
same-bind-credentials
```

Mode

LDAP Server

Description

Enable using same bind credentials as the server that this is the backup for.

Example

same-bind-credentials

Syntax

no same-bind-credentials

Mode

LDAP Server

Description

Disable using same bind credentials as the server that this is the backup for.

Example

no same-bind-credentials

Syntax

schema { custom | inet-org-person | microsoft-active-directory | network-information-service | novell-edirectory | samba-smb }

Mode

LDAP Server

Description

Configure the LDAP schema.

Options

<i>custom</i>	Configure the schema manually.
<i>inet-org-person</i>	Use the pre-configured RFC-2798 InetOrgPerson schema.
<i>microsoft-active-directory</i>	Use the pre-configured Microsoft Active Directory schema.
<i>network-information-service</i>	Use the pre-configured RFC-2307 Network Information Service schema.
<i>novell-edirectory</i>	Use the pre-configured Novell eDirectory schema.
<i>samba-smb</i>	Use the pre-configured Samba SMB schema.

Example

schema samba-smb
schema microsoft-active-directory
schema novell-edirectory

Syntax

read-from-server auto-configure [servers]

Mode

LDAP Schema

Description

Read the schema from the LDAP server and auto-configure the local schema to match.

Options

servers Automatically update the schema configuration on all servers.

Example

```
read-from-server auto-configure
read-from-server auto-configure servers
```

Syntax

```
read-from-server display
```

Mode

LDAP Schema

Description

Read the schema from the LDAP server and display it.

Example

```
read-from-server display
```

Syntax

```
user-class <WORD>
```

Mode

LDAP Schema

Description

Set the class name of user objects.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-class user
```

Syntax

```
user-attribute { additional-group-id <WORD> | framed-ip-address <WORD> | group-membership <WORD> | logon-name <WORD> |
qualified-logon-name <WORD> | use-additional-group-id }
```

Mode

LDAP Schema

Description

Define attributes of user objects.

Options

additional-group-id	Set the additional user group ID attribute.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

<i>framed-ip-address</i>	Set the framed IP address attribute.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>group-membership</i>	Set the user group membership attribute.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>logon-name</i>	Set the user logon name attribute.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>qualified-logon-name</i>	Set the qualified logon name attribute.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>use-additional-group-id</i>	Use the additional user group ID attribute.

Example

```
user-attribute logon-name myuid
user-attribute qualified-logon-name myUserPrincipalName
user-attribute group-membership myMemberOf
user-attribute additional-group-id myPrimaryGroupID
user-attribute use-additional-group-id
user-attribute framed-ip-address myFramedIPAddress
```

Syntax

```
no user-attribute { additional-group-id | framed-ip-address | group-membership | logon-name | qualified-logon-name | use-
additional-group-id }
```

Mode

LDAP Schema

Description

Remove attributes of user objects.

Options

<i>additional-group-id</i>	Remove the additional user group ID attribute.
<i>framed-ip-address</i>	Remove the framed IP address attribute.
<i>group-membership</i>	Remove the user group membership attribute.
<i>logon-name</i>	Remove the user logon name attribute.
<i>qualified-logon-name</i>	Remove the qualified logon name attribute.
<i>use-additional-group-id</i>	Do not use the additional user group ID attribute.

Example

```
no user-attribute logon-name
no user-attribute qualified-logon-name
no user-attribute group-membership
no user-attribute additional-group-id
no user-attribute use-additional-group-id
no user-attribute framed-ip-address
```

Syntax

```
user-group-class <WORD>
```

Mode

Description

Set the class name of user group objects.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-group-class groupOfNames

Syntax

user-group-attribute { additional-group-match <WORD> | member { distinguished-name | user-id } <WORD> }

Mode

Description

Define attributes of user group objects.

Options

additional-group-match Set the additional user group match attribute.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

member Set the name/type of the member attribute.

distinguished-name The member attribute holds a distinguished name.

user-id The member attribute holds a user ID (uid).
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-group-attribute member user-id memberId
user-group-attribute member distinguished-name memberId
user-group-attribute additional-group-match myPrimaryGroupToken

Syntax

no user-group-attribute { additional-group-match | member }

Mode

Description

Remove attributes of user group objects.

Options

additional-group-match Remove the additional user group match attribute.

member Remove the name of the member attribute.

Example

no user-group-attribute member
no user-group-attribute additional-group-match

Syntax

directory

Mode

LDAP Server

Description

Configure the LDAP directory.

Example

directory

Syntax

read-trees-from-server [domain <WORD>] { append | replace } { add | ignore }

Mode

LDAP Directory

Description

Read the directory trees containing users and user groups from the LDAP server.

Options

- domain** The domain to search under.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- append** Append to existing trees.
- replace** Replace existing trees.
- add** For append method, we need append trees found on that server to\n its own configuration, and for replace method, we need to replace\n the trees in that server's own configuration with those found on it.
- ignore** Ignore trees found on that server.

Example

```
read-trees-from-server append add
read-trees-from-server append ignore
read-trees-from-server replace add
read-trees-from-server replace ignore
read-trees-from-server domain mydomain.com append add
```

Syntax

primary-domain <WORD>

Mode

LDAP Directory

Description

Set the primary LDAP domain.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
primary-domain mydomain.com
```

Syntax

```
no primary-domain
```

Mode

LDAP Directory

Description

Remove the primary LDAP domain.

Example

```
no primary-domain
```

Syntax

```
users-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Add or re-order a directory tree to search in when searching for user objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
users-tree mydomain.com/users
users-tree ou=users,dc=mydomain,dc=com
```

Syntax

```
no users-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Remove a directory tree to search in when searching for user objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
no users-tree mydomain.com/users
no users-tree ou=users,dc=mydomain,dc=com
```

Syntax

```
no users-trees
```

Mode

LDAP Directory

Description

Remove all directory trees to search in when searching for user objects.

Example

```
no users-trees
```

Syntax

```
user-groups-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Add or re-order a directory tree to search in when searching for user group objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
user-groups-tree mydomain.com/groups
user-groups-tree ou=groups,dc=mydomain,dc=com
```

Syntax

```
no user-groups-tree <LDAP_DIRECTORY_NAME>
```

Mode

LDAP Directory

Description

Remove a directory tree to search in when searching for user group objects.

Options

<LDAP_DIRECTORY_NAME> LDAP directory user or group name.
Example: *abc*

Example

```
no user-groups-tree mydomain.com/groups
no user-groups-tree ou=groups,dc=mydomain,dc=com
```

Syntax

```
no user-groups-trees
```

Mode

LDAP Directory

Description

Remove all directory trees to search in when searching for user group objects.

Example

```
no user-groups-trees
```

Syntax

```
bind { anonymous | distinguished-name <WORD> | name <WORD> { location <WORD> } }
```

Mode

LDAP Server

Description

Set how to bind to the LDAP server, either selecting anonymous bind, giving the full distinguished name to use, or giving the account name to use and its location in the directory tree (the latter can be in either URL or DN format).

Options

<i>anonymous</i>	Bind anonymously.
<i>distinguished-name</i>	Set the full distinguished name to use.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>name</i>	Set the account name to use.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>location</i>	Set the account location in the directory tree.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
bind name administrator location builtin
bind distinguished-name "cn=name,ou=User,dc=mydomain,dc=com"
bind anonymous
```

Syntax

```
bind-password <ENC_PASSWORD>
```

Mode

LDAP Server

Description

Set the password for binding to the LDAP server.

Options

<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>

Example

```
bind-password mypassword
```

Syntax

```
no bind-password
```

Mode

LDAP Server

Description

Clear the password for binding to the LDAP server.

Example

```
no bind-password
```

Syntax

```
referred-bind-with-account { local | other-servers }
```

Mode

LDAP Server

Description

Set the bind method when referred to other servers.

Options

local	Bind with this account.
other-servers	Bind with an equivalent account on that server (same password).

Example

```
referred-bind-with-account local
referred-bind-with-account other-servers
```

Syntax

```
test <LDAP_SERVER_HOST_NAME> type { connectivity-bind | ldap-search [ return-attribute <WORD> ] { { basic <WORD> use { group { member | name } | user { common-name | login-name | qualified-name } } } | filter <WORD> { base { other <WORD> | root-directory | top-domain-tree } scope { base-entry-only | level-below-base | subtree } } } } | user-authentication <WORD> <WORD> [ chap ] }
```

Mode

LDAP

Description

Run the LDAP test to the specified server with one type of test.

Options

<LDAP_SERVER_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i>
type	Select one test type.
connectivity-bind	Connectivity/bind test. This test will simply try to bind to the LDAP server with the configured bind credentials.
ldap-search	LDAP search test. This test will have basic and advanced modes.
return-attribute	The return attributes will allow specifying a list of the attributes to return and display rather than displaying the entire matched entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
basic	Search for a user or a group.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
use	
group	Search for a group with a given name or member.
member	Search for a group with specific member.
name	Search for a group with specific group name.

user	Search for a user with a given login name or common name.
common-name	Search for a user with specific common name.
login-name	Search for a user with specific login name.
qualified-name	Search for a user with specific qualified login name.
filter	Set the search filter for advanced mode.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
base	Set the search base.
other	Other search base.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
root-directory	Root of the directory.
top-domain-tree	Top of the domain tree.
scope	Set the search scope.
base-entry-only	Search the base entry only.
level-below-base	Search one level below the base.
subtree	Search the sub-tree.
user-authentication	User authentication test, testing that a given user name and password can be sent to and authenticated by the LDAP server.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
chap	Test LDAP in a CHAP-compatible way.

Example

```
test 192.168.168.15 type connectivity-bind
test 192.168.168.15 type user-authentication adminUser password
test 192.168.168.15 type user-authentication adminUser password chap
test 192.168.168.15 type ldap-search user login-name adminUser
test 192.168.168.15 type ldap-search group name adminGroup
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent base root-directory scope subtree
test 192.168.168.15 type ldap-search filter LDAPTestFilterContent base other "dc=example,dc=com" scope subtree
test 192.168.168.15 type ldap-search return-attri dn user login-name adminUser
test 192.168.168.15 type ldap-search return-attri cn group name adminGroup
test 192.168.168.15 type ldap-search return-attri cn filter LDAPTestFilterContent
test 192.168.168.15 type ldap-search return-attri dn filter LDAPTestFilterContent base root-directory scope subtree
test 192.168.168.15 type ldap-search return-attri dn filter LDAPTestFilterContent base other "dc=example,dc=com" scope subtree
```

Syntax

```
import type { user-detail | user-group | user-list } from { all | server <LDAP_SERVER_HOST_NAME> }
```

Mode

LDAP

Description

import user or user group from ldap server.

Options

type	import type.
user-detail	Import user detail.
user-group	Import user group.

<i>user-list</i>	Import user group.
<i>from</i>	import source.
<i>all</i>	import from all servers.
<i>server</i>	import server.
<i><LDAP_SERVER_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i>

Example

```
import type group from all
import type group from server 10.21.49.22
import type group from partition mypartition
import type user-detail from all
import type user-list from server 11.11.17.17
```

Syntax

```
user sso
```

Mode

Config

Description

Configure SSO settings.

Example

```
user sso
```

Syntax

```
clear user sso statistics [ agent <SSO_AGENT_HOST_NAME> | global | radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> |
terminal-services-agent <SSO_TS_AGENT_HOST_NAME> | third-party-api-client <SSO_3RD_PARTY_API_CLIENT_HOST> ]
```

Mode

SSO
Top Level
Config

Description

Reset SSO statistics.

Options

<i>agent</i>	Reset SSO agent statistics.
<i><SSO_AGENT_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i>
<i>global</i>	Reset global (non-agent) SSO statistics.
<i>radius-accounting-client</i>	Reset SSO RADIUS accounting client statistics.
<i><SSO_RAD_ACCT_CLIENT_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
<i>terminal-services-agent</i>	Reset SSO terminal services agent statistics.
<i><SSO_TS_AGENT_HOST_NAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i>
<i>third-party-api-client</i>	Reset SSO third party api client statistics.
<i><SSO_3RD_PARTY_API_CLIENT_HOST></i>	SSO third party api client host name. Example: <i>abc</i>

Example


```
clear user sso statistics
```

Syntax

```
method { browser-ntlm [ { after-sso-agent-failed | before-sso-agent | enabled } ] | capture-client | radius-accounting | sso-agent | terminal-services-agent | third-party-api }
```

Mode

SSO

Description

Enable the single-sign-on mechanism.

Options

<i>browser-ntlm</i>	Enable browser NTLM authentication.
<i>after-sso-agent-failed</i>	Use NTLM to authenticate HTTP traffic only if SSO via the agent fails.
<i>before-sso-agent</i>	Use NTLM to authenticate HTTP traffic before attempting SSO via the agent.
<i>enabled</i>	Enable browser-ntlm option.
<i>capture-client</i>	Enable capture-client authentication.
<i>radius-accounting</i>	Enable RADIUS accounting authentication.
<i>sso-agent</i>	Enable SSO agent authentication.
<i>terminal-services-agent</i>	Enable terminal services agent authentication.
<i>third-party-api</i>	Enable third party api authentication.

Example

```
method sso-agent
```

Syntax

```
no method { browser-ntlm | capture-client | radius-accounting | sso-agent | terminal-services-agent | third-party-api }
```

Mode

SSO

Description

Disable the single-sign-on mechanism.

Options

<i>browser-ntlm</i>	Disable browser NTLM authentication.
<i>capture-client</i>	Enable capture-client authentication.
<i>radius-accounting</i>	Disable RADIUS accounting authentication.
<i>sso-agent</i>	Disable SSO agent authentication.
<i>terminal-services-agent</i>	Disable terminal services agent authentication.
<i>third-party-api</i>	Enable third party api authentication.

Example

```
no method sso-agent
```

Syntax

```
next-agent-on-no-name
```

Mode

SSO

Description

Enable try next agent on getting no name from NetAPI/WMI.

Example

```
next-agent-on-no-name
```

Syntax

```
no next-agent-on-no-name
```

Mode

SSO

Description

Disable try next agent on getting no name from NetAPI/WMI.

Example

```
no next-agent-on-no-name
```

Syntax

```
block-traffic
```

Mode

SSO

Description

Block user traffic while waiting for SSO.

Example

```
block-traffic
```

Syntax

```
no block-traffic
```

Mode

SSO

Description

Disable block user traffic while waiting for SSO.

Example

```
no block-traffic
```

Syntax

```
including-for-access-rules { all | selected }
```

Mode

SSO

Description

Allow through user traffic for all or selected access rules.

Options

all Allow through user traffic for all access rules.

selected Allow through user traffic for all access rules.

Example

```
including-for-access-rules all
```

Syntax

```
no including-for-access-rules
```

Mode

SSO

Description

Block user traffic for all access rules.

Example

```
no including-for-access-rules
```

Syntax

```
sync-all-agents-user-db
```

Mode

SSO

Description

Sync all agents when agent synchronize their user databases.

Example

```
sync-all-agents-user-db
```

Syntax

```
no sync-all-agents-user-db
```

Mode

SSO

Description

Sync those with the same user identification mechanisms when agent synchronize their user databases.

Example

```
no sync-all-agents-user-db
```

Syntax

```
local-users-only
```

Mode

SSO

Description

Limit login to only SSO users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

```
no local-users-only
```

Mode

SSO

Description

Disable limit login to only SSO users with accounts in the local user database.

Example

```
no local-users-only
```

Syntax

```
non-domain-limited-access
```

Mode

SSO

Description

Allow limited access for users who are identified by SSO but reported by the agent as not logged into the domain. These users will not be given membership to the Trusted Users user group (even when set locally).

Example

```
non-domain-limited-access
```

Syntax

```
no non-domain-limited-access
```

Mode

SSO

Description

Disable allow any access for users who are reported by the agent as not logged into the domain.

Example

```
no non-domain-limited-access
```

Syntax

```
probe { netapi [ [ over-netbios | over-tcp ] ] | test-mode | timeout <UINT16> | wmi }
```

Mode

SSO

Description

Probe IP addresses to check if they respond to NetAPI or WMI before making an SSO attempt
 Set timeout for probing IP addresses
 Enable probe test-mode.

Options

netapi	Probe for NetAPI, default over NetBIOS.
over-netbios	Probe for NetAPI over NetBIOS.
over-tcp	Probe for NetAPI over TCP.
test-mode	Enable probe test-mode. Probe test mode allows testing that SSO probes are functioning correctly during SSO without their interfering with the user authentications
timeout <UINT16>	Set timeout for probing IP addresses. Integer in the form: D OR 0xHHHH. Example: 123
wmi	Probe for WMI.

Example

```
probe netapi over-tcp
probe wmi
probe time-out 5
probe test-mode
```

Syntax

```
no probe [ test-mode ]
```

Mode

SSO

Description

Disable probe IP addresses to check if they respond to NetAPI or WMI before making an SSO attempt.

Options

test-mode Disable probe test-mode.

Example

```
no probe
```

Syntax

```
user-group-mechanism { ldap | local-only }
```

Mode

SSO

Description

Set the mechanism to use to set user group memberships for users who are authenticated via SSO.

Options

ldap Read user groups via LDAP.

local-only Set using local users that duplicate SSO users.

Example

```
user-group-mechanism ldap
```

Syntax

```
poll rate <UINT32>
```

Mode

SSO

Description

Set the polling rate for checking if logged in users who were identified via SSO are still logged in.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
poll rate 10
```

Syntax

```
poll same-agent
```

Mode

SSO

Description

Enable poll the same agent that authenticated the user.

Example

```
poll same-agent
```

Syntax

```
no poll same-agent
```

Mode

SSO

Description

Disable poll the same agent that authenticated the user.

Example

```
no poll same-agent
```

Syntax

hold-time after-failure <UINT16>

Mode

SSO

Description

Set the time to hold off from trying again to identify the user at an IP address following an SSO failure for it.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

hold-time after-failure 10

Syntax

hold-time after-no-user <UINT16>

Mode

SSO

Description

Set the time to hold off from trying again to identify the user at an IP address following reporting no user for it.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

hold-time after-no-user 10

Syntax

ramp-up rate <UINT8>

Mode

SSO

Description

Enable ramp up and set the rate.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

ramp-up rate 1

Syntax

no ramp-up

Mode

SSO

Description

Disable ramp up.

Example

no ramp-up

Syntax

user-domain-name { consistent | received }

Mode

SSO

Description

When different SSO resource report different name variant for a user domain.

Options

consistent Use consistent domain name

received Use received domain name.

Example

user-domain-name received

Syntax

windows-service-user-name <WINDOWS_SERVICE_USER_NAME>

Mode

SSO

Description

Add a name to the list of user names known to be used by Windows services (and so to be ignored by the SSO agent).

Options

<WINDOWS_SERVICE_USER_NAME> The login name of a windows service.
Example: *abc*

Example

windows-service-user-name someservice

Syntax

no windows-service-user-name <WINDOWS_SERVICE_USER_NAME>

Mode

SSO

Description

Remove a name from the list of user names known to be used by Windows services (and so to be ignored by the SSO agent).

Options

<WINDOWS_SERVICE_USER_NAME> The login name of a windows service.
Example: *abc*

Example

no windows-service-user-name someservice

Syntax

no windows-service-user-names

Mode

SSO

Description

Remove all names from the list of user names known to be used by Windows services (and so to be ignored by the SSO agent).

Example

no windows-service-user-names

Syntax

name <WINDOWS_SERVICE_USER_NAME>

Mode

SSO windows service user

Description

name.

Options

<WINDOWS_SERVICE_USER_NAME> The login name of a windows service.
Example: *abc*

Example

name user1

Syntax

security-service-bypass address { [ipv6] { { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <SECURITY_SERVICE_BYPASS_IP_NAME> }

Mode

SSO

Description

Add/edit one bypass SSO rule for the specified address(es).

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i>	Host address object.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

network	Network address object.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Range address object.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Group address object name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<SECURITY_SERVICE_BYPASS_IP_NAME>	Security service bypass IP name. Example: <i>Web Server</i>

Example

```
security-service-bypass address name "Non-User Addresses"
```

Syntax

```
no security-service-bypass address { group <ADDR_GROUP_NAME_MIXED> | name <SSO_BYPASS_ADDRESS_NAME> }
```

Mode

SSO

Description

Delete one bypass rule with specified address.

Options

group	Service group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Service object name.
<SSO_BYPASS_ADDRESS_NAME>	SSO bypass rule address name. Example: <i>abc</i>

Example

```
no security-service-bypass address "Non-User Addresses"
```

Syntax

```
security-service-bypass service { built-in <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | group <SVC_GROUP_NAME> | name <SSO_BYPASS_SERVICE_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

SSO

Description

Add/edit one bypass SSO rule for the specified service(s).

Options

<i>built-in</i>	SSO bypass built-in service object.
<i><SSO_BYPASS_SERVICE_BUILT_IN_NAME></i>	SSO bypass built-in object name. Example: <i>abc</i>
<i>group</i>	Service group name.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<i><SSO_BYPASS_SERVICE_NAME></i>	SSO bypass rule service name. Example: <i>abc</i>
<i>protocol</i>	Service protocol.
<i><SVC_PROTOCOL></i>	Service protocol. Example: <i>TCP</i>
<i><SVC_PORT_BEGIN></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i><SVC_PORT_END></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
security-service-bypass service name "POP3"
```

Syntax

```
no security-service-bypass service { group <SSO_BYPASS_SERVICE_NAME> | name <SSO_BYPASS_SERVICE_NAME> }
```

Mode

SSO

Description

Delete one bypass rule with specified service.

Options

<i>group</i>	Service group name.
<i><SSO_BYPASS_SERVICE_NAME></i>	SSO bypass rule service name. Example: <i>abc</i>
<i>name</i>	Service object name.
<i><SSO_BYPASS_SERVICE_NAME></i>	SSO bypass rule service name. Example: <i>abc</i>

Example

```
no security-service-bypass service name "POP3"
```

Syntax

```
address { [ ipv6 ] { { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <SECURITY_SERVICE_BYPASS_IP_NAME> }
```

Mode

SSO Bypass

Description

Set address object or group as bypass rule name.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i>	Host address object.

<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Network address object.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Range address object.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Group address object name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<SECURITY_SERVICE_BYPASS_IP_NAME>	Security service bypass IP name. Example: <i>Web Server</i>

Example

```
address name ssoBypassName
```

Syntax

```
service { built-in <SSO_BYPASS_SERVICE_BUILT_IN_NAME> | group <SVC_GROUP_NAME> | name <SSO_BYPASS_SERVICE_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

SSO Bypass

Description

Set service object or group as bypass rule name.

Options

built-in	SSO bypass built-in service object.
<SSO_BYPASS_SERVICE_BUILT_IN_NAME>	SSO bypass built-in object name. Example: <i>abc</i>
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SSO_BYPASS_SERVICE_NAME>	SSO bypass rule service name. Example: <i>abc</i>
protocol	Service protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
service name ssoBypassName
```

Syntax

```
type { full-bypass | trigger-sso }
```

Mode

SSO Bypass

Description

Set bypass type.

Options

full-bypass Set bypass type as full bypass.

trigger-sso Set bypass type as trigger SSO but bypass holding packets while waiting for it.

Example

```
type full-bypass
```

Syntax

```
log-user-name <WORD>
```

Mode

SSO

Description

SSO bypass user name for logging.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
log testname create-dummy-user timeout 10
```

Syntax

```
no log-user-name
```

Mode

SSO

Description

Do not log SSO bypass user name.

Example

```
no log-user-name
```

Syntax

```
dummy-user { enable | name <WORD> | timeout <UINT16> }
```

Mode

SSO

Description

Enable create dummy user entries for SSO bypass and set its configuration.

Options

- enable** Enable create dummy user entries for SSO bypass.
- name** Set user name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- timeout** Set inactivity timeout.
- <UINT16>** Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
dummy-user enable
dummy-user name "SSO Bypass"
dummy-user timeout 15
```

Syntax

```
no dummy-user { enable | name }
```

Mode

SSO

Description

Disable create dummy user entries for SSO bypass or clear user name.

Options

- enable** Disable Dummy User.
- name** Clear user name.

Example

```
no dummy-user
no dummy-user name
```

Syntax

```
enforce-on-zone <SSO_ZONE_NAME>
```

Mode

SSO

Description

Select to always enforce SSO on a zone.

Options

- <SSO_ZONE_NAME>** Zone object name.
Example: *DMZ*

Example

```
enforce-on-zone lan
```

Syntax

```
no enforce-on-zone <SSO_ZONE_NAME>
```

Mode

SSO

Description

Select to not always enforce SSO on a zone.

Options

<SSO_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

```
no enforce-on-zone lan
```

Syntax

```
bypass-policy { dhcp | ipsec | ospf | rip | voip }
```

Mode

SSO

Description

Auto-create per-zone security policies for the specified service to bypass SSO enforcement.

Options

dhcp Auto-create SSO bypass security policies for DHCP.

ipsec Auto-create SSO bypass security policies for IPSec.

ospf Auto-create SSO bypass security policies for OSPF.

rip Auto-create SSO bypass security policies for RIP.

voip Auto-create SSO bypass security policies for VOIP.

Example

```
bypass-policy voip
```

Syntax

```
no bypass-policy { dhcp | ipsec | ospf | rip | voip }
```

Mode

SSO

Description

Don't auto-create per-zone security policies for the specified service to bypass SSO enforcement.

Options

dhcp Don't auto-create SSO bypass security policies for DHCP.

ipsec Don't auto-create SSO bypass security policies for IPSec.

ospf Don't auto-create SSO bypass security policies for OSPF.

rip Don't auto-create SSO bypass security policies for RIP.

voip Don't auto-create SSO bypass security policies for VOIP.

Example

no bypass-policy voip

Syntax

tlsa-services-bypass

Mode

SSO

Description

Allow traffic from services on a terminal server running the TS agent to bypass user authentication in access rules.

Example

tlsa-services-bypass

Syntax

no tlsa-services-bypass

Mode

SSO

Description

Don't Allow traffic from services on a terminal server running the TS agent to bypass user authentication in access rules.

Example

no tlsa-services-bypass

Syntax

authentication-domain { custom <WORD> | inherit-from-ldap }

Mode

SSO

Description

Set the authentication domain.

Options

- custom** User the custom domain.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- inherit-from-ldap** User the domain from the LDAP configuration.

Example

authentication-domain custom "www.mydomain.com"

Syntax


```
redirect-browser { certificate-name | domain-name { { configured | reverse-dns-look-up } } | ip-address }
```

Mode

SSO

Description

Set method of redirect browser to SonicWall appliance's own web server.

Options

<i>certificate-name</i>	Via the name from the administration certificate
<i>domain-name</i>	Via the domain name
<i>configured</i>	Via its configured domain name
<i>reverse-dns-look-up</i>	Via its domain name from a reverse DNS lookup of the interface IP address
<i>ip-address</i>	Via the interface IP address

Example

```
redirect-browser ip-address
```

Syntax

```
retries-on-failure <UINT16>
```

Mode

SSO

Description

Set maximum retries to allow on authentication failure.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
retries-on-failure 3
```

Syntax

```
poll users { linux | macintosh | windows } { { agent | bypass-re-authentication | re-authentication-ntlm } }
```

Mode

SSO

Description

On the poll timer, set polling method for users authenticated via NTLM in different system.

Options

<i>linux</i>	Set polling method for linux users.
<i>macintosh</i>	Set polling method for macintosh users.
<i>windows</i>	Set polling method for windows users.
<i>agent</i>	Poll via the SSO agent.

bypass-re-authentication Don't re-authenticate.

re-authentication-ntlm Re-authenticate via NTLM.

Example

```
poll users linux re-authentication-ntlm
```

Syntax

```
forward-lanman
```

Mode

SSO

Description

Enable forward legacy LanMan in NTLM.

Example

```
forward-lanman
```

Syntax

```
no forward-lanman
```

Mode

SSO

Description

Disable forward legacy LanMan in NTLM.

Example

```
no forward-lanman
```

Syntax

```
radius-accounting-port <IPV4_PORT>
```

Mode

SSO

Description

Set the RADIUS accounting's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
radius-accounting-port 1813
```

Syntax

```
radius-acct-lookup-mechanism { from-radius-acct-requests | selected-on-sso-user-tab }
```

Mode

SSO

Description

Mechanism for looking up user group memberships for RADIUS Accounting users.

Options

from-radius-acct-requests Use Filter-Id attribute from RADIUS Accounting requests.

selected-on-sso-user-tab Use the mechanism selected on the SSO Users tab.

Example

```
radius-acct-lookup-mechanism selected-on-sso-user-tab
```

Syntax

```
switch-over-time <UINT32>
```

Mode

SSO

Description

Expect Start/Stop messages due to wireless roaming. Maximum switch-over time.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
switch-over-time 30
```

Syntax

```
no switch-over-time
```

Mode

SSO

Description

Expect Start/Stop messages due to wireless roaming. Maximum switch-over time.

Example

```
no switch-over-time
```

Syntax

```
ignore-transition-message
```

Mode

SSO

Description

Ignore transition message sequence/source(s).

Example

Syntax

```
no ignore-transition-message
```

Mode

SSO

Description

Expect logical transitions.

Example

```
no ignore-transition-message
```

Syntax

```
ignore-addr { group <ADDR_GROUP_NAME> | name <ADDR_NAME> | none }
```

Mode

SSO

Description

Ignore any RADIUS Accounting messages when users at these IP addresses.

Options

group	address group name.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
name	address object name.
<ADDR_NAME>	Address object name. Example: <i>Web Server</i>
none	Do not ignore any object.

Example

```
ignore-addr name "ALL XO Managemetn IP"
```

Syntax

```
include-addr { all | group <ADDR_GROUP_NAME> | name <ADDR_NAME> }
```

Mode

SSO

Description

Include any RADIUS Accounting messages when users at these IP addresses.

Options

all	All address objects and groups.
group	address group name.
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>

<i>name</i>	address object name.
<i><ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>

Example

```
include-addr name "ALL X0 Managemetrn IP"
```

Syntax

```
radius-user-name-exclusion <SSO_RAD_ACCT_USER_NAME_EXCL_MATCH> type { begin | end }
```

Mode

SSO

Description

Add RADIUS accounting user name exclusion.

Options

<i><SSO_RAD_ACCT_USER_NAME_EXCL_MATCH></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>type</i>	type
<i>begin</i>	begin.
<i>end</i>	end.

Example

```
radius-user-name-exclusion name1
```

Syntax

```
no radius-user-name-exclusion <SSO_RAD_ACCT_USER_NAME_EXCL_MATCH> type { begin | end }
```

Mode

SSO

Description

Delete RADIUS accounting user name exclusion.

Options

<i><SSO_RAD_ACCT_USER_NAME_EXCL_MATCH></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>type</i>	type
<i>begin</i>	begin.
<i>end</i>	end.

Example

```
no radius-user-name-exclusion name1
```

Syntax

```
no radius-user-name-exclusions
```

Mode

SSO

Description

Delete all RADIUS accounting user name exclusion.

Example

```
no radius-user-name-exclusions
```

Syntax

```
name <SSO_RAD_ACCT_USER_NAME_EXCL_MATCH>
```

Mode

SSO RADIUS accounting user name match exclusion

Description

RADIUS accounting user name exclusion.

Options

<SSO_RAD_ACCT_USER_NAME_EXCL_MATCH> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name user1
```

Syntax

```
type { begin | end }
```

Mode

SSO RADIUS accounting user name match exclusion

Description

.

Options

begin begin.

end end.

Example

```
type begin
```

Syntax

```
agent <SSO_AGENT_HOST_NAME>
```

Mode

SSO

Description

Configure an SSO agent.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
agent 192.168.168.1
```

Syntax

```
no agent <SSO_AGENT_HOST_NAME>
```

Mode

SSO

Description

Delete an SSO agent.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
no agent 192.168.168.1
```

Syntax

```
no agents
```

Mode

SSO

Description

Delete all SSO agents.

Example

```
no agents
```

Syntax

```
host <SSO_AGENT_HOST_NAME>
```

Mode

SSO Agent

Description

Set the SSO agent's host name or IP address.

Options

<SSO_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Agent*

Example

```
host 192.168.168.1
```

Syntax

```
port <IPV4_PORT>
```

Mode

SSO Agent

Description

Set the SSO agent's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 389

Syntax

enable

Mode

SSO Agent

Description

Enable the SSO agent.

Example

enable

Syntax

no enable

Mode

SSO Agent

Description

Disable the SSO agent.

Example

no enable

Syntax

timeout <UINT16>

Mode

SSO Agent

Description

Set the timeout on replies from the agent.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

timeout 10

Syntax

retries <UINT16>

Mode

SSO Agent

Description

Set the maximum number of retries to make after timeouts waiting for replies from the agent.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

retries 10

Syntax

no shared-key

Mode

SSO Agent

Description

Clear the shared key for encrypting messages to/from the agent.

Example

no shared-key

Syntax

shared-key <ENC_HEX_STRING>

Mode

SSO Agent

Description

Set the hexadecimal value of the shared key for encrypting messages to/from the SSO agent.

Options

<ENC_HEX_STRING> String of hexadecimal digits.
Example: 0123456989abcdef

Example

shared-key 1234abcd

Syntax

max-requests <UINT16>

Mode

SSO Agent

Description

Set the maximum number of requests to send to the agent at a time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-requests 10
```

Syntax

```
terminal-services-agent <SSO_TS_AGENT_HOST_NAME>
```

Mode

SSO

Description

Configure a terminal services agent.

Options

<SSO_TS_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Terminal-Services-Agent*

Example

```
terminal-services-agent 192.168.168.1
```

Syntax

```
no terminal-services-agent <SSO_TS_AGENT_HOST_NAME>
```

Mode

SSO

Description

Delete a terminal services agent.

Options

<SSO_TS_AGENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *SSO-Terminal-Services-Agent*

Example

```
no terminal-services-agent 192.168.168.1
```

Syntax

```
no terminal-services-agents
```

Mode

SSO

Description

Delete all terminal services agents.

Example

no terminal-services-agents

Syntax

host <HOSTNAME>

Mode

SSO Agent

Description

Set the agent's host name or IP address.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

host 192.168.168.1

Syntax

port <IPV4_PORT>

Mode

SSO Agent

Description

Set the agent's UDP port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 389

Syntax

enable

Mode

SSO Agent

Description

Enable the terminal services agent.

Example

enable

Syntax

no enable

Mode

SSO Agent

Description

Disable the terminal services agent.

Example

```
no enable
```

Syntax

```
no shared-key
```

Mode

SSO Agent

Description

Clear the shared key for encrypting messages to/from the agent.

Example

```
no shared-key
```

Syntax

```
shared-key <ENC_HEX_STRING>
```

Mode

SSO Agent

Description

Set the hexadecimal value of the shared key for encrypting messages to/from the terminal services agent.

Options

<ENC_HEX_STRING> String of hexadecimal digits.
Example: *0123456989abcdef*

Example

```
shared-key 1234abcd
```

Syntax

```
radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO

Description

Configure a RADIUS accounting client.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
radius-accounting-client 192.168.168.11
```

Syntax

```
no radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO

Description

Delete a RADIUS accounting client.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
no radius-accounting-client 192.168.168.11
```

Syntax

```
no radius-accounting-clients
```

Mode

SSO

Description

Delete all RADIUS accounting clients.

Example

```
no radius-accounting-clients
```

Syntax

```
host <SSO_RAD_ACCT_CLIENT_HOST_NAME>
```

Mode

SSO RADIUS Accounting Client

Description

Set the RADIUS accounting client's host name or IP address.

Options

<SSO_RAD_ACCT_CLIENT_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
host 192.168.168.1
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

SSO RADIUS Accounting Client

Description

Set the value of the shared secret for encrypting messages to/from the client.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

shared-secret 1234abcd

Syntax

no shared-secret

Mode

SSO RADIUS Accounting Client

Description

Clear the shared secret for encrypting messages to/from the client.

Example

no shared-secret

Syntax

user-name-format { canonical | custom <WORD> | down-level-logon | sonicwall-aventail | user-name | user-principle }

Mode

SSO RADIUS Accounting Client

Description

Set user name attribute format.

Options

<i>canonical</i>	Set to pre-defined \"Domain/User-name\" format.
<i>custom</i>	Set to pre-defined custom format.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>down-level-logon</i>	Set to pre-defined \"Domain\\User-name\" format.
<i>sonicwall-aventail</i>	Set to pre-defined \"SonicWall Aventail\" format.
<i>user-name</i>	Set to pre-defined \"User-name\" format.
<i>user-principle</i>	Set to pre-defined \"User-name@Domain\" format.

Example

user-name-format user-name

Syntax

custom-format-components component1 { dn | domain | not-use | user-name }

Mode

SSO RADIUS Accounting Client

Description

Components for user name attribute format.

Options

<i>dn</i>	Specify dn as the component.
<i>domain</i>	Specify domain as the component.
<i>not-use</i>	Don't use this component.
<i>user-name</i>	Specify user-name as the component.

Example

```
name-format component1 user-name
```

Syntax

```
custom-format-components component2 { dn | domain | not-use | user-name }
```

Mode

SSO RADIUS Accounting Client

Description

Components for user name attribute format.

Options

<i>dn</i>	Specify dn as the component.
<i>domain</i>	Specify domain as the component.
<i>not-use</i>	Don't use this component.
<i>user-name</i>	Specify user-name as the component.

Example

```
name-format component2 user-name
```

Syntax

```
custom-format-components component3 { dn | domain | not-use | user-name }
```

Mode

SSO RADIUS Accounting Client

Description

Components for user name attribute format.

Options

<i>dn</i>	Specify dn as the component.
<i>domain</i>	Specify domain as the component.
<i>not-use</i>	Don't use this component.
<i>user-name</i>	Specify user-name as the component.

Example

name-format component1 user-name

Syntax

missing-domain { ldap-look-up | local-user }

Mode

SSO RADIUS Accounting Client

Description

Set approach if the domain component is missing in a RADIUS message.

Options

ldap-look-up Look up the user name via LDAP.

local-user Assume a non-domain user.

Example

missing-domain ldap-look-up

Syntax

log-user-out-if-no-interim { auto | enable }

Mode

SSO RADIUS Accounting Client

Description

Log user out if no interim updates are received.

Options

auto Auto

enable Enable.

Example

log-user-out-if-no-interim enable

Syntax

no log-user-out-if-no-interim enable

Mode

SSO RADIUS Accounting Client

Description

Do not Log user out if no interim updates are received.

Options

enable Enable.

Example

log-user-out-if-no-interim enable

Syntax

log-user-out-timeout <UINT32>

Mode

SSO RADIUS Accounting Client

Description

Log user out if no accounting interim updates are received for the specified minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

log-user-out 5

Syntax

no log-user-out-timeout

Mode

SSO RADIUS Accounting Client

Description

Disable log user out.

Example

no log-user-out

Syntax

server <SSO_RAD_ACCT_FORWARD_SERVER_ID> <SSO_RAD_ACCT_PROXY_FWD_SERVER_HOST_NAME> [*port* <IPV4_PORT>] [*shared-secret* <ENC_PASSWORD>]

Mode

SSO RADIUS Accounting Client

Description

Configure the server for receiving RADIUS accounting messages forwarded from this client.

Options

<SSO_RAD_ACCT_FORWARD_SERVER_ID>	Integer in the form: D OR 0xHH. Example: 1
<SSO_RAD_ACCT_PROXY_FWD_SERVER_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
<i>port</i>	Set the server's port number.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: 80
<i>shared-secret</i>	Set the shared secret.
<ENC_PASSWORD>	Password. Example: <i>secret</i>

Example

server 1 192.168.168.11 port 1813 shared-secret 123abc

Syntax

```
no server <SSO_RAD_ACCT_FORWARD_SERVER_ID> [ shared-secret ]
```

Mode

SSO RADIUS Accounting Client

Description

Clear a RADIUS accounting client forwarding server.

Options

<SSO_RAD_ACCT_FORWARD_SERVER_ID>	Integer in the form: D OR 0xHH. Example: <i>1</i>
shared-secret	Clear the shared secret.

Example

```
no server 1
```

Syntax

```
proxy-forward timeout <UINT16>
```

Mode

SSO RADIUS Accounting Client

Description

Set timeout for each forward.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
proxy-forward timeout 5
```

Syntax

```
proxy-forward retries <UINT16>
```

Mode

SSO RADIUS Accounting Client

Description

Set retries number for each accounting server.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
proxy-forward retries 5
```

Syntax

```
proxy-forward type { forward-to-all | try-next-on-timeout }
```

Mode

Description

Set how to proxy forward to multiple accounting servers.

Options

forward-to-all Proxy forward to all servers.

try-next-on-timeout Try next server when timeout.

Example

```
proxy-forward type try-next-on-timeout
```

Syntax

```
consistent-domain-name <SSO_CONS_DOMAIN_NAME_DN>
```

Mode

SSO

Description

Set the name variant to use for specific domain.

Options

<SSO_CONS_DOMAIN_NAME_DN> User domain name use - DN.
Example: *dc=mydomain,dc=com*

Example

```
consistent-domain-name dc=mydomain,dc=com
```

Syntax

```
no consistent-domain-name <SSO_CONS_DOMAIN_NAME_DN>
```

Mode

SSO

Description

Unset the name variant to use for specific domain.

Options

<SSO_CONS_DOMAIN_NAME_DN> User domain name use - DN.
Example: *dc=mydomain,dc=com*

Example

```
no consistent-domain-name dc=mydomain,dc=com
```

Syntax

```
no consistent-domain-names
```

Mode

SSO

Description

Unset the name variant to use for all domains.

Example

no consistent-domain-names

Syntax

dn <SSO_CONS_DOMAIN_NAME_DN>

Mode

Consistent domain name

Description

User domain name use - DN.

Options

<SSO_CONS_DOMAIN_NAME_DN> User domain name use - DN.
Example: *dc=mydomain,dc=com*

Example

dn dc=mydomain,dc=com

Syntax

name <SSO_CONS_DOMAIN_NAME_NAME>

Mode

Consistent domain name

Description

User domain name use - name.

Options

<SSO_CONS_DOMAIN_NAME_NAME> User domain name use - Name.
Example: *mydomain.com*

Example

name MYDOMAIN

Syntax

no name

Mode

Consistent domain name

Description

User domain name use - name.

Example

no name

Syntax

```
test [ agent <SSO_AGENT_HOST_NAME> [ user-ip <IPV4_HOST> [ mechanism { allow-both | from-3rd-party-api | from-domain-controller | from-exchange-server | from-novell-server | from-other-mechanisms | from-terminal-server | via-netapi-or-wmi } ] ] | terminal-services-agent <SSO_TS_AGENT_HOST_NAME> ]
```

Mode

SSO

Description

Run the SSO test with the given user name/password.

Options

agent	Specify an agent to test.
<SSO_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i>
user-ip	The IP address of a user to test.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
mechanism	User Identification Mechanisms.
allow-both	Allow both.
from-3rd-party-api	From agent's 3rd-party API.
from-domain-controller	From domain controllers.
from-exchange-server	From microsoft exchange server.
from-novell-server	From novell server.
from-other-mechanisms	From other mechanisms.
from-terminal-server	From terminal server.
via-netapi-or-wmi	Via NetAPI/WMI.
terminal-services-agent	Specify a terminal services agent to test.
<SSO_TS_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i>

Example

```
test agent 192.168.168.1 user-ip 192.168.168.99
```

Syntax

```
third-party-api
```

Mode

SSO

Description

Enter 3rd Party API configuration mode.

Example

```
third-party-api
```

Syntax

```
enable
```

Mode

Third Party API

Description

Enable SSO third party API.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Third Party API

Description

Disable SSO third party API.

Example

```
no enable
```

Syntax

```
https-port { management | number <IPV4_PORT> }
```

Mode

Third Party API

Description

Configure SSO third party API HTTPS port number.

Options

management Set SSO third party API HTTPS port number the same as HTTPS management port.

number Set SSO third party API HTTPS port numbert.

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
https-port number 12345
```

Syntax

```
client <SSO_3RD_PARTY_API_CLIENT_HOST>
```

Mode

Third Party API

Description

Configure an SSO third party API client.

Options

<SSO_3RD_PARTY_API_CLIENT_HOST> SSO third party api client host name.
Example: *abc*

Example

```
client 192.168.168.1
```

Syntax

```
no client <SSO_3RD_PARTY_API_CLIENT_HOST>
```

Mode

Third Party API

Description

Delete an SSO third party API client.

Options

<SSO_3RD_PARTY_API_CLIENT_HOST> SSO third party api client host name.
Example: *abc*

Example

```
no client 192.168.168.1
```

Syntax

```
no clients
```

Mode

Third Party API

Description

Delete all SSO third party API clients.

Example

```
no clients
```

Syntax

```
host <SSO_3RD_PARTY_API_CLIENT_HOST>
```

Mode

SSO Third Party API Client

Description

Set the 3rd party api client's host name or IP address.

Options

<SSO_3RD_PARTY_API_CLIENT_HOST> SSO third party api client host name.
Example: *abc*

Example

```
host 192.168.168.1
```

Syntax

```
enable
```

Mode

Description

Enable the SSO third party API client.

Example

enable

Syntax

no enable

Mode

SSO Third Party API Client

Description

Disable the SSO third party API client.

Example

no enable

Syntax

authentication-type { both | certificate | shared-secret }

Mode

SSO Third Party API Client

Description

Set authentication type for API client.

Options

- both*** Set authentication type for API client to use both shared secret and certificate.
- certificate*** Set authentication type for API client to certificate.
- shared-secret*** Set authentication type for API client to shared secret.

Example

authentication-type shared-secret

Syntax

shared-secret <ENC_PASSWORD>

Mode

SSO Third Party API Client

Description

Set the shared secret for API client.

Options

- <ENC_PASSWORD>*** Password.
Example: *secret*

Example

```
shared-secret passwd
```

Syntax

```
no shared-secret
```

Mode

SSO Third Party API Client

Description

Clear the shared secret for API client.

Example

```
no shared-secret
```

Syntax

```
security-level { high { allow-all | sha256 | sha512 } | low | medium }
```

Mode

SSO Third Party API Client

Description

Set shared secret verification security level.

Options

high	High.
allow-all	Both SHA512 and SHA256.
sha256	SHA256.
sha512	SHA512.
low	Low (no shared secret verification).
medium	Medium (SHA256 but no replay prevention).

Example

```
security-level high sha256
```

Syntax

```
replay-prevention
```

Mode

SSO Third Party API Client

Description

Enable CSRF/replay prevention.

Example

```
replay-prevention
```

Syntax

no replay-prevention

Mode

SSO Third Party API Client

Description

Disable CSRF/replay prevention.

Example

no replay-prevention

Syntax

origin-restriction allowed <WORD>

Mode

SSO Third Party API Client

Description

Enable restriction of origins if client uses CORS.

Options

- allowed*** Configure allowed origins.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

origin-restriction

Syntax

no origin-restriction

Mode

SSO Third Party API Client

Description

Disable restriction of origins if client uses CORS.

Example

no origin-restriction

Syntax

persistent-connections

Mode

SSO Third Party API Client

Description

Enable allow persistent connections.

Example

persistent-connections

Syntax

no persistent-connections

Mode

SSO Third Party API Client

Description

Disable allow persistent connections.

Example

no persistent-connections

Syntax

capture-client

Mode

SSO

Description

Enter Capture Client configuration mode.

Example

capture-client

Syntax

enable

Mode

Capture Client Enforcement

Description

Enable SSO Capture Client.

Example

enable

Syntax

no enable

Mode

Capture Client Enforcement

Description

Disable SSO Capture Client.

Example

no enable

Syntax

user guest

Mode

Config

Description

Configure settings related to guest users.

Example

user guest

Syntax

profile <GUEST_PROFILE_NAME>

Mode

Guest User

Description

Add or update a guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

profile "Custom Profile"

Syntax

no profile <GUEST_PROFILE_NAME>

Mode

Guest User

Description

Delete a guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

no profile "Custom Profile"

Syntax

user [uuid] <GUEST_USER_NAME> [password <ENC_PASSWORD> [hide-password]]

Mode

Guest User

Description

Add or edit a guest user account.

Options

<i>uuid</i>	Edit a user object by UUID.
<i><GUEST_USER_NAME></i>	Guest user name. Example: <i>guest1</i>
<i>password</i>	Set the guest user password.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>
<i>hide-password</i>	Don't show the auto-generated password.

Example

```
user johndoe
user johndoe password password
user johndoe password password hide-password
```

Syntax

```
generate
```

Mode

Guest User

Description

Auto generate some guest users.

Example

```
generate 2
```

Syntax

```
num <UINT32>
```

Mode

Guest User Generate

Description

Auto generate some guest users.

Options

<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
num 2
```

Syntax

```
no user [ uuid ] <GUEST_USER_NAME>
```

Mode

Guest User

Description

Delete a guest user account.

Options

<i>uuid</i>	Delete a user object by UUID.
<i><GUEST_USER_NAME></i>	Guest user name.

Example: *guest1*

Example

```
no user johndoe
```

Syntax

```
no users <WORD>
```

Mode

Guest User

Description

Delete all guest user accounts with a given name prefix.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no users temp-guest
```

Syntax

```
show-guest-status-window
```

Mode

Guest User

Description

Enable showing the login status window after guest login.

Example

```
show-guest-status-window
```

Syntax

```
no show-guest-status-window
```

Mode

Guest User

Description

Disable showing the login status window after guest login.

Example

```
no show-guest-status-window
```

Syntax

```
export guest-accounts { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Description

Export guest accounts' configurations.

Options

- ftp**

Export using the FTP protocol.
- <FTP_URL>**

FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\: ', '@' -> '\\@ ', '/' -> '\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*
- scp**

Export using the SCP protocol.
- <SCP_URL>**

SCP URL in the form: userName@serverip:/fileDirectory.
Example: *userTest@10.10.10.10:/home/userTest/*
- port**

SCP server port
- <IPV4_PORT>**

Integer in the form: D OR 0xHHHH.
Example: *80*

Example

export guest-accounts ftp ftp://user:password@servername/ guest-accounts.csv

Syntax

logout guest at <GUEST_LOGIN_USER_BY_IP>

Mode

Description

Logout guest user.

Options

- at**

Logout a guest user by IP.
- <GUEST_LOGIN_USER_BY_IP>**

IPV4: address in the form: D.D.D.D\\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\\n.
Example: *2001:cdba:0000:0000:0000:0000:3257:9652*

Example

logout gyst at 192.168.168.1

Syntax

logout guests

Mode

Description

Logout guest users.

Example

logout guests

Syntax

```
name <GUEST_PROFILE_NAME>
```

Mode

Guest Profile

Description

Set the name of the guest user profile.

Options

<GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*

Example

```
name profile1
```

Syntax

```
generate { name | password }
```

Mode

Guest Profile

Description

Auto generate names or passwords for guest accounts created with this profile.

Options

name Auto-generate names for created guest accounts.

password Auto generate passwords for created guest accounts.

Example

```
generate name
generate password
```

Syntax

```
no generate { name | password }
```

Mode

Guest Profile

Description

Disable auto generate names or passwords for guest accounts created with this profile.

Options

name Disable auto-generate names for created guest accounts.

password Disable auto generate passwords for created guest accounts.

Example

```
no generate name
no generate password
```

Syntax

name-prefix <WORD>

Mode

Guest Profile
Guest User Generate

Description

Set a prefix for auto generated names for guest accounts created with this profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name-prefix guest

Syntax

comment <WORD>

Mode

Guest Profile
Guest User Generate

Description

Set comment for guest accounts created with this profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Added via profile1"

Syntax

no comment

Mode

Guest Profile
Guest User Generate

Description

Clear comment for guest accounts created with this profile.

Example

no comment

Syntax

enable

Mode

Guest Profile
Guest User Generate

Description

Enable guest accounts to be created.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Guest Profile
Guest User Generate

Description

Disable guest accounts to be created.

Example

```
no enable
```

Syntax

```
activate-on-login
```

Mode

Guest Profile
Guest User Generate

Description

Enable activate account upon first login.

Example

```
activate-on-login
```

Syntax

```
no activate-on-login
```

Mode

Guest Profile
Guest User Generate

Description

Disable activate account upon first login.

Example

```
no activate-on-login
```

Syntax

```
login-uniqueness
```

Mode

Guest Profile
Guest User Generate

Description

Enable enforcing unique login sessions.

Example

login-uniqueness

Syntax

no login-uniqueness

Mode

Guest Profile
Guest User Generate

Description

Disable enforcing unique login sessions.

Example

no login-uniqueness

Syntax

prune-on-expiry

Mode

Guest Profile
Guest User Generate

Description

Enable to delete the guest accounts when they are expired if a limited lifetime is set.

Example

prune-on-expiry

Syntax

no prune-on-expiry

Mode

Guest Profile
Guest User Generate

Description

Disable to delete the guest accounts when they are expired.

Example

no prune-on-expiry

Syntax

account-lifetime { days <UINT16> | hours <UINT16> | minutes <UINT16> }

Mode

Guest Profile
Guest User Generate

Description

Set a limited lifetime for the guest accounts.

Options

- days**

Set the lifetime in days.
- <UINT16>**

Integer in the form: D OR 0xHHHH.
Example: 123
- hours**

Set the lifetime in hours.
- <UINT16>**

Integer in the form: D OR 0xHHHH.
Example: 123
- minutes**

Set the lifetime in minutes.
- <UINT16>**

Integer in the form: D OR 0xHHHH.
Example: 123

Example

account-lifetime hours 20

Syntax

no quota-cycle

Mode

- Guest Profile
- Guest User Generate

Description

Set no quota cycle for the guest accounts created with this profile.

Example

no quota-cycle

Syntax

quota-cycle { day | month | week }

Mode

- Guest Profile
- Guest User Generate

Description

Set a quota cycle for the guest accounts created with this profile.

Options

- day**

Set the quota cycle as one day.
- month**

Set the quota cycle as one month.
- week**

Set the quota cycle as one week.

Example

quota-cycle per day

Syntax

session-lifetime { days <UINT16> | hours <UINT16> | minutes <UINT16> }

Mode

Guest Profile
Guest User Generate

Description

Set a session time limit for the created guest accounts.

Options

- days

Set the session limit in days.
- <UINT16>

Integer in the form: D OR 0xHHHH.
Example: 123
- hours

Set the session limit in hours.
- <UINT16>

Integer in the form: D OR 0xHHHH.
Example: 123
- minutes

Set the session limit in minutes.
- <UINT16>

Integer in the form: D OR 0xHHHH.
Example: 123

Example

session-lifetime hours 23

Syntax

idle-timeout { days <UINT32> | hours <UINT32> | minutes <UINT32> }

Mode

Guest Profile
Guest User Generate

Description

Set the session inactivity timeout for created guest accounts.

Options

- days

Set the idle timeout in days.
- <UINT32>

Integer in the form: D OR 0xHHHHHHHHH.
Example: 123
- hours

Set the idle timeout in hours.
- <UINT32>

Integer in the form: D OR 0xHHHHHHHHH.
Example: 123
- minutes

Set the idle timeout in minutes.
- <UINT32>

Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

idle-timeout minutes 20

Syntax

limit { receive <UINT32> | transmit <UINT32> }

Mode

Guest Profile
Guest User Generate

Description

Set the receive or transmit limit in MB.

Options

receive Set the receive limit in MB.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

transmit Set the transmit limit in MB.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
limit receive 500
limit transmit 300
```

Syntax

```
no limit { receive | transmit }
```

Mode

Guest Profile
Guest User Generate

Description

Disable receive or transmit limit.

Options

receive Disable receive limit.

transmit Disable transmit limit.

Example

```
no limit receive
no limit transmit
```

Syntax

```
name <GUEST_USER_NAME>
```

Mode

Guest User

Description

Set the login name of the guest account.

Options

<GUEST_USER_NAME> Guest user name.
Example: *guest1*

Example

```
name johndoe
```

Syntax

```
uuid <UUID>
```

Mode

Guest User

Description

Set user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0500-c0eae49ce84c

Syntax

no uuid <UUID>

Mode

Guest User

Description

Clear user object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

no uuid

Syntax

generate { name | password [hide] }

Mode

Guest User

Description

Generate a login name or password for the guest account.

Options

name Generate a login name for the guest account.

password Generate a password for the guest account.

hide Disable showing the generated password.

Example

generate name
generate password

Syntax

```
profile <GUEST_PROFILE_NAME> [ hide-password ]
```

Mode

Guest User

Description

Enable the settings from a guest profile.

Options

- <GUEST_PROFILE_NAME> Guest profile name.
Example: *profile1*
- hide-password* Disable showing the auto-generated password.

Example

```
profile "Custom Profile"
```

Syntax

```
comment <WORD>
```

Mode

Guest User

Description

Set comment for the guest account.

Options

- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Added 7/26/2010"
```

Syntax

```
no comment
```

Mode

Guest User

Description

Clear the comment for the guest account.

Example

```
no comment
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

Guest User

Description

Set the guest account password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password pwd1234

Syntax

no password

Mode

Guest User

Description

Clear the guest account password.

Example

no password

Syntax

enable

Mode

Guest User

Description

Enable the guest account.

Example

enable

Syntax

no enable

Mode

Guest User

Description

Disable the guest account.

Example

no enable

Syntax

activate-on-login

Mode

Guest User

Description

Enable activate account upon first login.

Example

```
activate-on-login
```

Syntax

```
no activate-on-login
```

Mode

Guest User

Description

Disable activate account upon first login.

Example

```
no activate-on-login
```

Syntax

```
login-uniqueness
```

Mode

Guest User

Description

Enable enforcing a unique login session with the guest account.

Example

```
login-uniqueness
```

Syntax

```
no login-uniqueness
```

Mode

Guest User

Description

Disable enforcing a unique login session with the guest account.

Example

```
no login-uniqueness
```

Syntax

```
prune-on-expiry
```

Mode

Guest User

Description

Enable delete the guest account when it is expired if a limited lifetime is set.

Example

prune-on-expiry

Syntax

no prune-on-expiry

Mode

Guest User

Description

Disable delete the guest account when it is expired.

Example

no prune-on-expiry

Syntax

account-lifetime { days <UINT16> | hours <UINT16> | minutes <UINT16> }

Mode

Guest User

Description

Set a limited lifetime for the guest account.

Options

days Set the lifetime in days.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

hours Set the lifetime in hours.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

minutes Set the lifetime in minutes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

account-lifetime hours 22

Syntax

no quota-cycle

Mode

Guest User

Description

Set no quota cycle for the guest account.

Example

no quota-cycle

Syntax

```
quota-cycle { day | month | week }
```

Mode

Guest User

Description

Set a quota cycle for the guest account.

Options

day Set the quota cycle as one day.

month Set the quota cycle as one month.

week Set the quota cycle as one week.

Example

```
quota-cycle per day
```

Syntax

```
session-lifetime { days <UINT16> | hours <UINT16> | minutes <UINT16> }
```

Mode

Guest User

Description

Set a session time limit for the guest account.

Options

days Set the session limit in days.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

hours Set the session limit in hours.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

minutes Set the session limit in minutes.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
session-lifetime hours 23
```

Syntax

```
no session-lifetime
```

Mode

Guest User

Description

Disable session time limit for the guest account.

Example

```
no session-lifetime
```

Syntax

```
idle-timeout { days <UINT32> | hours <UINT32> | minutes <UINT32> }
```

Mode

Guest User

Description

Set the session inactivity timeout for the guest account.

Options

days	Set the idle timeout in days.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
hours	Set the idle timeout in hours.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
minutes	Set the idle timeout in minutes.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
idle-timeout minutes 20
```

Syntax

```
limit { receive <UINT32> | transmit <UINT32> }
```

Mode

Guest User

Description

Set the receive or transmit limit in MB for the guest account.

Options

receive	Set the receive limit in MB for the guest account.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
transmit	Set the transmit limit in MB for the guest account.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
limit receive 500  
limit transmit 300
```

Syntax

```
no limit { receive | transmit }
```

Mode

Guest User

Description

Disable receive or transmit limit for the guest account.

Options

receive Disable receive limit for the guest account.

transmit Disable transmit limit for the guest account.

Example

```
no limit receive
no limit transmit
```

Syntax

```
user tacacs
```

Mode

Config

Description

Configure TACACS settings.

Example

```
user tacacs
```

Syntax

```
local-users-only
```

Mode

TACACS

Description

Limit login to only TACACS users with accounts in the local user database.

Example

```
local-users-only
```

Syntax

```
no local-users-only
```

Mode

TACACS

Description

Disable limit login to only TACACS users with accounts in the local user database.

Example

```
no local-users-only
```

Syntax

```
user-group-mechanism { ldap | local-only }
```

Mode

TACACS

Description

Set the mechanism to use to set user group memberships for users who are authenticated via TACACS.

Options

- ldap** Read user groups via LDAP.
- local-only** Set using local users that duplicate TACACS users.

Example

```
user-group-mechanism ldap
```

Syntax

```
default-user-group <LOCAL_USER_GROUP_NAME>
```

Mode

TACACS

Description

Select a user group to whom all users who are authenticated via TACACS will be given membership by default (i.e. a group that can be used to set accesses etc. that will apply to all TACACS users).

Options

- <LOCAL_USER_GROUP_NAME>** Local user group object name.
Example: *Limited Administrators*

Example

```
default-user-group "TACACS Users"
```

Syntax

```
no default-user-group
```

Mode

TACACS

Description

TACACS will not be given membership to any user group by default.

Example

```
no default-user-group
```

Syntax

```
timeout <UINT32>
```

Mode

TACACS

Description

Set the timeout on replies from the TACACS+ servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
timeout 10
```

Syntax

```
retries <UINT32>
```

Mode

TACACS

Description

Set the maximum number of retries to make after timeouts waiting for replies from the TACACS+ servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
retries 10
```

Syntax

```
no retries
```

Mode

TACACS

Description

Never retries to make after timeouts waiting for replies from the TACACS+ servers.

Example

```
no retries
```

Syntax

```
single-connect
```

Mode

TACACS

Description

Enable support for single connect.

Example

```
single-connect
```

Syntax

no single-connect

Mode

TACACS

Description

Disable support for single connect.

Example

no single-connect

Syntax

periodic-check

Mode

TACACS

Description

Enable periodic check of TACACS servers that are down.

Example

periodic-check

Syntax

no periodic-check

Mode

TACACS

Description

Disable periodic check of TACACS servers that are down.

Example

no periodic-check

Syntax

server <TACACS_SERVER_HOST_NAME>

Mode

TACACS

Description

Configure an TACACS+ server.

Options

<TACACS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.tacacsServer.com*

Example

server 192.168.168.1

Syntax

```
no server <TACACS_SERVER_HOST_NAME>
```

Mode

TACACS

Description

Delete an TACACS+ server.

Options

<TACACS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.tacacsServer.com*

Example

```
no server 192.168.168.1
```

Syntax

```
no servers
```

Mode

TACACS

Description

Delete all TACACS+ servers.

Example

```
no servers
```

Syntax

```
host <TACACS_SERVER_HOST_NAME>
```

Mode

TACACS Server

Description

Set the TACACS server's host name or IP address.

Options

<TACACS_SERVER_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.tacacsServer.com*

Example

```
host 192.168.168.1
```

Syntax

```
port <UINT16>
```

Mode

TACACS Server

Description

Set the TACACS server's port number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

port 49

Syntax

enable

Mode

TACACS Server

Description

Enable the TACACS server.

Example

enable

Syntax

no enable

Mode

TACACS Server

Description

Disable the TACACS server.

Example

no enable

Syntax

shared-secret <ENC_PASSWORD>

Mode

TACACS Server

Description

Set the shared secret for messages to/from the TACACS+ server.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

shared-secret 1234abcd

Syntax

no shared-secret

Mode

TACACS Server

Description

Clear the shared secret for messages to/from the TACACS+ server.

Example

no shared-secret

Syntax

through-vpn

Mode

TACACS Server

Description

Enable enforce send packet through vpn tunnel.

Example

through-vpn

Syntax

no through-vpn

Mode

TACACS Server

Description

Disable enforce send packet through vpn tunnel.

Example

no through-vpn

Syntax

test <TACACS_SERVER_HOST_NAME> [user <WORD> <WORD> [auth-method { chap | mschap | password-auth }]] [outbound] [combined] [clear-packet]

Mode

TACACS

Description

Run the TACACS test using specified server.

Options

<TACACS_SERVER_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.tacacsServer.com</i>
user	Run the TACACS user test with the given user name/password.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
auth-method	select a authentication method.
chap	Run the test with TACACS in CHAP mode.

<i>mschap</i>	Run the test with TACACS in MSCHAP mode.
<i>password-auth</i>	Run the test with TACACS in password authentication mode.
<i>outbound</i>	Run the test for outbound TACACS+ authentication.
<i>combined</i>	Run the test for combined AAA authentication.
<i>clear-packet</i>	Run the test by sending clear TACACS+ packet.

Example

```
test 192.168.168.16
test 192.168.168.16 user user1 pwd1234
```

Syntax

accounting

Mode

TACACS

Description

Configure TACACS accounting settings.

Example

accounting

Syntax

server <TACACS_ACCOUNTING_HOST_NAME>

Mode

TACACS Accounting

Description

Configure a TACACS accounting server.

Options

<TACACS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: 10.10.10.10\nwww.tacacsServer.com

Example

server 192.168.168.16

Syntax

no server <TACACS_ACCOUNTING_HOST_NAME>

Mode

TACACS Accounting

Description

Delete a TACACS accounting server.

Options

<TACACS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: 10.10.10.10\nwww.tacacsServer.com

Example

```
no server 192.168.168.16
```

Syntax

```
no servers
```

Mode

TACACS Accounting

Description

Delete all TACACS accounting servers.

Example

```
no servers
```

Syntax

```
enable
```

Mode

TACACS Accounting Server

Description

Enable the TACACS accounting server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

TACACS Accounting Server

Description

Disable the TACACS accounting server.

Example

```
no enable
```

Syntax

```
host <TACACS_ACCOUNTING_HOST_NAME>
```

Mode

TACACS Accounting Server

Description

Set the TACACS accounting server's host name or IP address.

Options

<TACACS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: `10.10.10.10\www.tacacsServer.com`

Example

```
host 192.168.168.1
```

Syntax

```
port <UINT16>
```

Mode

TACACS Accounting Server

Description

Set the TACACS accounting server's TCP port number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
port 1812
```

Syntax

```
shared-secret <ENC_PASSWORD>
```

Mode

TACACS Accounting Server

Description

Set the TACACS accounting server's shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
shared-secret mysecret
```

Syntax

```
no shared-secret
```

Mode

TACACS Accounting Server

Description

Clear the TACACS accounting server's shared secret.

Example

```
no shared-secret
```

Syntax

```
test <TACACS_ACCOUNTING_HOST_NAME>
```

Mode

TACACS Accounting

Description

Run the TACACS accounting server test using specified server.

Options

<TACACS_ACCOUNTING_HOST_NAME> Hostname in the form: hostname OR a.b.c.d.
Example: *10.10.10.10\www.tacacsServer.com*

Example

```
test 192.168.168.16
```

Syntax

```
timeout <UINT32>
```

Mode

TACACS Accounting

Description

Set the timeout for the TACACS accounting servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
timeout 10
```

Syntax

```
retries <UINT32>
```

Mode

TACACS Accounting

Description

Set the number of retries for the TACACS accounting servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
retries 10
```

Syntax

```
no retries
```

Mode

TACACS Accounting

Description

Set zero retries for the TACACS accounting servers.

Example

```
no retries
```

Syntax

```
single-connect
```

Mode

TACACS Accounting

Description

Enable support for single connect.

Example

```
single-connect
```

Syntax

```
no single-connect
```

Mode

TACACS Accounting

Description

Disable support for single connect.

Example

```
no single-connect
```

Syntax

```
packet-encrypted
```

Mode

TACACS Accounting

Description

Enable packet encrypted.

Example

```
packet-encrypted
```

Syntax

```
no packet-encrypted
```

Mode

TACACS Accounting

Description

Disable packet encrypted.

Example

no packet-encrypted

Syntax

```
data { guest | remote-client | sso-authenticated | sso-users-identified-via-radius-accounting | web-login }
```

Mode

TACACS Accounting

Description

Enable sending accounting data to servers or for users.

Options

<i>guest</i>	Enable sending accounting data for guest users.
<i>remote-client</i>	Enable sending accounting data for remote client users.
<i>sso-authenticated</i>	Enable sending accounting data for SSO-authenticated users.
<i>sso-users-identified-via-radius-accounting</i>	Enable including SSO users identified via RADIUS Accounting.
<i>web-login</i>	Enable sending accounting data for users authenticated by web login.

Example

```
data web-login
data remote-client
data guest
data sso-authenticated
data sso-users-identified-via-radius-accounting
```

Syntax

```
no data { guest | remote-client | sso-authenticated | sso-users-identified-via-radius-accounting | web-login }
```

Mode

TACACS Accounting

Description

Disable sending accounting data to servers or for users.

Options

<i>guest</i>	Disable sending accounting data for guest users.
<i>remote-client</i>	Disable sending accounting data for remote client users.
<i>sso-authenticated</i>	Disable sending accounting data for SSO-authenticated users.
<i>sso-users-identified-via-radius-accounting</i>	Disable including SSO users identified via RADIUS Accounting.
<i>web-login</i>	Disable sending accounting data for users authenticated by web login.

Example

```
no data web-login
no data remote-client
no data guest
no data sso-authenticated
no data sso-users-identified-via-radius-accounting
```

Syntax

```
include { domain-and-local-users | domain-users | local-users }
```

Mode

TACACS Accounting

Description

Include different users in user accounting.

Options

domain-and-local-users Include local and domain users in user accounting.

domain-users Include domain users in user accounting.

local-users Include local users in user accounting.

Example

```
include domain-users
include local-users
include domain-and-local-users
```

Syntax

```
watchdog-messages <UINT8>
```

Mode

TACACS Accounting

Description

Enable send watchdog messages.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
watchdog-messages
```

Syntax

```
no watchdog-messages
```

Mode

TACACS Accounting

Description

Disable send watchdog messages.

Example

```
no watchdog-messages
```

Syntax

```
show user authentication [ base | methods | rule-auth-bypass-http-urls ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show user authentication related settings.

Options

<i>base</i>	Show user authentication base settings.
<i>methods</i>	Show user authentication method and single sign on methods.
<i>rule-auth-bypass-http-urls</i>	Show user authentication bypass rules settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

show user authentication

Syntax

show user local [base | group { name | uuid } <LOCAL_GROUP_GROUP_NAME> [domain <LOCAL_GROUP_DOMAIN_NAME>] | groups | user { name | uuid } <LOCAL_USER_USER_NAME> [domain <LOCAL_USER_DOMAIN_NAME>] [status] | users [status]] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show settings for local users/groups.

Options

<i>base</i>	Show local users base settings.
<i>group</i>	Show a local user group.
<i>name</i>	Show a user group object by name.
<i>uuid</i>	Show a user group object by UUID.
<i><LOCAL_GROUP_GROUP_NAME></i>	User group object name. Example: <i>Limited Administrators</i>
<i>domain</i>	Set the user group's domain.
<i><LOCAL_GROUP_DOMAIN_NAME></i>	User group object domain name. Example: <i>example.com</i>
<i>groups</i>	Show all local user groups.
<i>user</i>	Show a local user.
<i>name</i>	Show a user object by name.
<i>uuid</i>	Show a user object by UUID.
<i><LOCAL_USER_USER_NAME></i>	User object name. Example: <i>John</i>
<i>domain</i>	Set the user's domain.
<i><LOCAL_USER_DOMAIN_NAME></i>	User object domain name. Example: <i>example.com</i>
<i>status</i>	Show a local user quota status.
<i>users</i>	Show all local users.
<i>status</i>	Show all local users quota status.

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show user local
show user local users
show user local user name jcool
show user local user uuid 00000000-0000-0001-0500-c0eae49ce84c
show user local groups
show user local group uuid 00000000-0000-0001-0600-c0eae49ce84c
show user local group name "Special Users"
```

Syntax

```
show user status [ active | at <USER_MIXED_ADDR> [ user <UINT32> ] | cli | inactive | name <USER_LOGIN_NAME> | unauthenticated ] [ pending ] [ logged-in ] [ locked-out ] [ account-locked-out ]
```

Mode

All Modes

Description

Show information on current users.

Options

<i>active</i>	Show information of active users.
<i>at</i>	Show detail of a user at a given IP address.
<i><USER_MIXED_ADDR></i>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: 2001:cdba:0000:0000:0000:0000:3257:9652
<i>user</i>	For Terminal Services users only, select the user at the IP address.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123
<i>cli</i>	Show the status of CLI login users.
<i>inactive</i>	Show information of inactive users.
<i>name</i>	Show information of the users with the given name
<i><USER_LOGIN_NAME></i>	A connected user's login name. Example: jdoe
<i>unauthenticated</i>	Show information of unauthenticated users.
<i>pending</i>	Include users currently being authenticated.
<i>logged-in</i>	Include logged in users.
<i>locked-out</i>	Include locked out users.
<i>account-locked-out</i>	Include locked out users.

Example

```
show user status
show user status at 192.168.168.1
```

Syntax

```
show user statistics
```

Mode

All Modes

Description

Show current user's statistics information.

Example

show user statistics

Syntax

show user management

Mode

All Modes

Description

Show user management configuration.

Example

show user management

Syntax

show user sessions statistics

Mode

All Modes

Description

Show users sessions statistics information.

Example

show user sessions statistics

Syntax

show user radius [[accounting [[base | server <RADIUS_ACCOUNTING_HOST_NAME> | servers | statistics [server <RADIUS_ACCOUNTING_HOST_NAME>]]] | base | server <RADIUS_SERVER_HOST_NAME> | servers | statistics [server <RADIUS_SERVER_HOST_NAME>]] [{ pending-config | with-pending-config }]]

Mode

All Modes

Description

Show RADIUS settings and statistics.

Options

<i>accounting</i>	Show settings for RADIUS accounting settings.
<i>base</i>	Show RADIUS accounting base settings.
<i>server</i> <i><RADIUS_ACCOUNTING_HOST_NAME></i>	Show RADIUS accounting server settings. Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>
<i>servers</i>	Show settings for all RADIUS accounting servers.
<i>statistics</i> <i>server</i> <i><RADIUS_ACCOUNTING_HOST_NAME></i>	Show RADIUS accounting server statistics. Show statistics for a specific RADIUS accounting server. Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>

base	Show RADIUS base settings.
server <RADIUS_SERVER_HOST_NAME>	Show RADIUS server settings. Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>
servers	Show settings for all RADIUS servers.
statistics server <RADIUS_SERVER_HOST_NAME>	Show RADIUS server statistics. Show RADIUS server statistics of mentioned server. Hostname in the form: hostname OR a.b.c.d. Example: <i>10.10.10.10\www.radiusServer.com</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show user radius
show user radius servers
show user radius server 192.168.168.168
show user radius accounting
show user radius accounting servers
show user radius accounting server 192.168.168.1
show user radius statistics
show user radius statistics server 10.10.10.10
```

Syntax

```
show user ldap [ [ base | exclude-tree <LDAP_EXCLUDE_TREE> | exclude-trees | relay | server <LDAP_SERVER_HOST_NAME> | servers ] [ { pending-config | with-pending-config } ] ] | dynamic-server <LDAP_DYNAMIC_SERVER_NAME> | dynamic-servers | statistics [ { dynamic-server <LDAP_DYNAMIC_SERVER_NAME> | dynamic-servers | global | server <LDAP_SERVER_HOST_NAME> | servers } ] ]
```

Mode

All Modes

Description

Show LDAP settings and statistics.

Options

base	Show LDAP base settings.
exclude-tree <LDAP_EXCLUDE_TREE>	Show exclude user groups. LDAP exclude tree. Example: <i>abc</i>
exclude-trees	Show exclude user groups.
relay	Show LDAP relay configuration.
server <LDAP_SERVER_HOST_NAME>	Show specified LDAP server settings. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i>
servers	Show all LDAP servers settings.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
dynamic-server <LDAP_DYNAMIC_SERVER_NAME>	Show status for a specific LDAP dynamic server. Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Dynamic-Server</i>
dynamic-servers	Show all LDAP dynamic servers status.

statistics	Show LDAP server statistics.
dynamic-server	Show statistics for a specific LDAP dynamic server.
<LDAP_DYNAMIC_SERVER_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Dynamic-Server</i>
dynamic-servers	Show all LDAP dynamic serverS statistics.
global	Show LDAP servers global statistics.
server	Show statistics for a specific LDAP server.
<LDAP_SERVER_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>LDAP-Server</i>
servers	Show all LDAP servers statistics.

Example

```
show user ldap show user ldap servers
show user ldap server 192.168.168.2
show user ldap relay
show user ldap statistics
show user ldap statistics global
show user ldap statistics server 10.10.10.10
show user ldap statistics dynamic-server 10.10.10.11
show user ldap statistics servers
show user ldap dynamic-servers
show user ldap dynamic-server 20.20.20.20
```

Syntax

```
show user sso [ agent <SSO_AGENT_HOST_NAME> | agents | base | capture-client [ { base } ] | consistent-domain-name
<SSO_CONS_DOMAIN_NAME_DN> | consistent-domain-names | enforce-on-zones | radius-accounting-client
<SSO_RAD_ACCT_CLIENT_HOST_NAME> | radius-accounting-clients | radius-user-name-exclusion <SSO_RAD_ACCT_USER_NAME_EXCL_MATCH>
type { begin | end } | radius-user-name-exclusions | security-services-bypass | statistics [ { agent <SSO_AGENT_HOST_NAME> |
agents | all | global | radius-accounting-client <SSO_RAD_ACCT_CLIENT_HOST_NAME> | radius-accounting-clients | terminal-
services-agent <SSO_TS_AGENT_HOST_NAME> | terminal-services-agents | third-party-api-client <SSO_3RD_PARTY_API_CLIENT_HOST> |
third-party-api-clients } ] | status | terminal-services-agent <SSO_TS_AGENT_HOST_NAME> | terminal-services-agents | third-
party-api [ { base | client <SSO_3RD_PARTY_API_CLIENT_HOST> | clients } ] | windows-service-user-name
<WINDOWS_SERVICE_USER_NAME> | windows-service-user-names ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSO settings, status or statistics.

Options

agent	Show SSO agent settings.
<SSO_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i>
agents	Show settings for all SSO agents.
base	Show SSO base settings.
capture-client	Show capture client settings.
base	Show capture client global setting.
consistent-domain-name	Show consistent domain name.
<SSO_CONS_DOMAIN_NAME_DN>	User domain name use - DN. Example: <i>dc=mydomain,dc=com</i>
consistent-domain-names	Show consistent domain name.
enforce-on-zones	Show SSO enforce-on-zone settings.
radius-accounting-client	Show SSO RADIUS accounting client settings.

<SSO_RAD_ACCT_CLIENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
radius-accounting-clients	Show settings for all SSO RADIUS accounting clients.
radius-user-name-exclusion	Show RADIUS accounting user name exclusion.
<SSO_RAD_ACCT_USER_NAME_EXCL_MATCH>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
type	type.
begin	type begin.
end	type end.
radius-user-name-exclusions	Show RADIUS accounting user name exclusions.
security-services-bypass	Show SSO security service bypass settings.
statistics	Show SSO statistics.
agent	Show statistics for an SSO agent.
<SSO_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Agent</i>
agents	Show statistics for all SSO agents.
all	Show all SSO statistics.
global	Show SSO global statistics.
radius-accounting-client	Show statistics for an SSO RADIUS accounting client.
<SSO_RAD_ACCT_CLIENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
radius-accounting-clients	Show statistics for all SSO RADIUS accounting clients.
terminal-services-agent	Show statistics for an SSO terminal services agent.
<SSO_TS_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i>
terminal-services-agents	Show statistics for all SSO terminal services agents.
third-party-api-client	Show statistics for third party api client.
<SSO_3RD_PARTY_API_CLIENT_HOST>	SSO third party api client host name. Example: <i>abc</i>
third-party-api-clients	Show statistics for all third party api clients.
status	Show SSO agent status.
terminal-services-agent	Show SSO terminal services agent settings.
<SSO_TS_AGENT_HOST_NAME>	Hostname in the form: hostname OR a.b.c.d. Example: <i>SSO-Terminal-Services-Agent</i>
terminal-services-agents	Show settings for all SSO terminal services agents.
third-party-api	Show third party api settings.
base	Show third party api global setting.
client	Show third party api client setting.
<SSO_3RD_PARTY_API_CLIENT_HOST>	SSO third party api client host name. Example: <i>abc</i>
clients	Show all third party api clients setting.
windows-service-user-name	Show SSO windows service user name settings.
<WINDOWS_SERVICE_USER_NAME>	The login name of a windows service. Example: <i>abc</i>

<i>windows-service-user-names</i>	Show SSO windows service user name settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show user sso
show user sso agents
show user sso agent 192.168.168.1
```

Syntax

```
show user guest [ [ base | profile <GUEST_PROFILE_NAME> | profiles | user [ uuid ] <GUEST_USER_NAME> | users ] [ { pending-
config | with-pending-config } ] | [ detail [ name <GUEST_USER_NAME> ] | statistic { ip <GUEST_LOGIN_USER_BY_IP> | name
<GUEST_USER_NAME> } | statistics | status [ ip <GUEST_LOGIN_USER_BY_IP> ] ] ]
```

Mode

All Modes

Description

Show settings for guest profiles/users.

Options

<i>base</i>	Show guest users base settings.
<i>profile</i> <i><GUEST_PROFILE_NAME></i>	Show a guest user profile. Guest profile name. Example: <i>profile1</i>
<i>profiles</i>	Show all guest user profiles.
<i>user</i> <i>uuid</i> <i><GUEST_USER_NAME></i>	Show a guest user. Show a user object by UUID. Guest user name. Example: <i>guest1</i>
<i>users</i>	Show all guest users.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>detail</i> <i>name</i> <i><GUEST_USER_NAME></i>	Show guest user(s) detail. Show guest user detail. Guest user name. Example: <i>guest1</i>
<i>statistic</i>	Show the logged-in guest users' statistic.
<i>ip</i> <i><GUEST_LOGIN_USER_BY_IP></i>	Show the logged-in guest user's statistic. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
<i>name</i> <i><GUEST_USER_NAME></i>	Show the guest user's statistic by name. Guest user name. Example: <i>guest1</i>
<i>statistics</i>	Show the guest user's statistics.
<i>status</i> <i>ip</i>	Show the logged-in guest users' status. Show the logged-in guest user's status.

<GUEST_LOGIN_USER_BY_IP> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
show user guest
show user guest users
show user guest user uuid 00000000-0000-0001-0500-c0eae49ce84c
show user guest user jcool
```

Syntax

```
show user tacacs [ [ accounting [ [ base | server <TACACS_ACCOUNTING_HOST_NAME> | servers | statistics [ server
<TACACS_ACCOUNTING_HOST_NAME> ] ] ] | base | server <TACACS_SERVER_HOST_NAME> | servers | statistics [ server
<TACACS_SERVER_HOST_NAME> ] ] [ { pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show TACACS settings.

Options

accounting	Show settings for TACACS accounting settings.
base	Show TACACS accounting base settings.
server <TACACS_ACCOUNTING_HOST_NAME>	Show TACACS accounting server settings. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\nwww.tacacsServer.com
servers	Show settings for all RADIUS accounting servers.
statistics server <TACACS_ACCOUNTING_HOST_NAME>	Show TACACS accounting server statistics. Show statistics for a specific TACACS accounting server. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\nwww.tacacsServer.com
base	Show TACACS base settings.
server <TACACS_SERVER_HOST_NAME>	Show TACACS server settings. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\nwww.tacacsServer.com
servers	Show settings for all TACACS servers.
statistics server <TACACS_SERVER_HOST_NAME>	Show TACACS server statistics. Show TACACS server statistics of mentioned server. Hostname in the form: hostname OR a.b.c.d. Example: 10.10.10.10\nwww.tacacsServer.com
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show user tacacs
show user tacacs servers
show user tacacs server 192.168.168.168
show user tacacs statistics
show user tacacs statistics server 192.168.168.4
show user tacacs accounting
show user tacacs accounting servers
show user tacacs accounting server 192.168.168.1
show user tacacs accounting statistics
show user tacacs accounting statistics server 192.168.168.3
```

Syntax

appflow

Mode

Config

Description

Enter appflow configuration mode.

Example

appflow

Syntax

clear flow-reporting statistics

Mode

AppFlow

Description

Clear flow reporting statistics.

Example

clear flow-reporting statistics

Syntax

default

Mode

AppFlow

Description

Clear all settings to default configuration.

Example

default

Syntax

report connections { all | interface-based | rules-based }

Mode

AppFlow

Description

Set the type of connections to report.

Options

all All connections.

interface-based Interface based.

rules-based Firewall/app rules based.

Example

```
report connections rules-based
report connections interface-based
report connections all
```

Syntax

```
real-time data-collection
```

Mode

AppFlow

Description

Enable real-time data collection.

Example

```
real-time data-collection
```

Syntax

```
no real-time data-collection
```

Mode

AppFlow

Description

Disable real-time data collection.

Example

```
no real-time data-collection
```

Syntax

```
real-time collect-for { [ top-applications ] [ bits-per-second ] [ packets-per-second ] [ average-packet-size ] [ connections-per-second ] [ core-utilization ] [ interface-protocols ] [ memory-utilization ] }
```

Mode

AppFlow

Description

Enable what to collect real-time data for.

Options

top-applications	Top applications.
bits-per-second	Bits per second.
packets-per-second	Packets per second.
average-packet-size	Average packet size.
connections-per-second	Connections per second.
core-utilization	Core utilization.
interface-protocols	Interface Protocols.
memory-utilization	Memory utilization.

Example

```
real-time collect-for top-apps core-utilization
```

Syntax

```
no real-time collect-for { [ top-applications ] [ bits-per-second ] [ packets-per-second ] [ average-packet-size ] [ connections-per-second ] [ core-utilization ] [ interface-protocols ] [ memory-utilization ] }
```

Mode

AppFlow

Description

Disable what to collect real-time data for.

Options

<i>top-applications</i>	Top applications.
<i>bits-per-second</i>	Bits per second.
<i>packets-per-second</i>	Packets per second.
<i>average-packet-size</i>	Average packet size.
<i>connections-per-second</i>	Connections per second.
<i>core-utilization</i>	Core utilization.
<i>interface-protocols</i>	Interface Protocols.
<i>memory-utilization</i>	Memory utilization.

Example

```
no real-time collect-for top-apps core-utilization
```

Syntax

```
aggregate data-collection
```

Mode

AppFlow

Description

Enable aggregate appflow report data collection.

Example

```
aggregate data-collection
```

Syntax

```
no aggregate data-collection
```

Mode

AppFlow

Description

Disable aggregate appflow report data collection.

Example

```
no aggregate data-collection
```

Syntax

```
aggregate collect-for { [ applications ] [ user ] [ ip ] [ threat ] [ geo-ip ] [ url ] }
```

Mode

AppFlow

Description

Enable what to collect aggregate report data for.

Options

<i>applications</i>	Applications report.
<i>user</i>	User report.
<i>ip</i>	Ip report.
<i>threat</i>	Threat report.
<i>geo-ip</i>	Geo-IP report.
<i>url</i>	URL report.

Example

```
aggregate collect-for applications user
```

Syntax

```
no aggregate collect-for { [ applications ] [ user ] [ ip ] [ threat ] [ geo-ip ] [ url ] }
```

Mode

AppFlow

Description

Disable what to collect aggregate report data for.

Options

<i>applications</i>	Applications report.
<i>user</i>	User report.
<i>ip</i>	Ip report.
<i>threat</i>	Threat report.
<i>geo-ip</i>	Geo-IP report.
<i>url</i>	URL report.

Example

```
no aggregate collect-for applications user
```

Syntax

```
flows-to local-collector
```

Mode

AppFlow

Description

Enable sending appflow to local collector.

Example

```
flows-to local-collector
```

Syntax

```
no flows-to local-collector
```

Mode

AppFlow

Description

Disable sending appflow to local collector.

Example

```
no flows-to local-collector
```

Syntax

```
report dropped
```

Mode

AppFlow

Description

Enable report dropped connection.

Example

```
report dropped
```

Syntax

```
no report dropped
```

Mode

AppFlow

Description

Disable report dropped connection.

Example

```
no report dropped
```

Syntax

```
report stack
```

Mode

AppFlow

Description

Enable report STACK connection.

Example

```
report stack
```

Syntax

```
no report stack
```

Mode

AppFlow

Description

Skip reporting STACK connection.

Example

no report stack

Syntax

```
include-url-types { [ gifs ] [ jpegs ] [ pngs ] [ js ] [ xmls ] [ jsons ] [ css ] [ htmls ] [ aspx ] [ cms ] }
```

Mode

AppFlow

Description

Enable inclusion of specified URL types.

Options

<i>gifs</i>	Gifs.
<i>jpegs</i>	Jpegs.
<i>pngs</i>	Pngs.
<i>js</i>	Js.
<i>xmls</i>	Xmls.
<i>jsons</i>	Jsons.
<i>css</i>	Css.
<i>htmls</i>	Htmls.
<i>aspx</i>	Aspx.
<i>cms</i>	Cms.

Example

```
include-url-types jpegs htmls
```

Syntax

```
no include-url-types { [ gifs ] [ jpegs ] [ pngs ] [ js ] [ xmls ] [ jsons ] [ css ] [ htmls ] [ aspx ] [ cms ] }
```

Mode

AppFlow

Description

Disable inclusion of specified URL types.

Options

<i>gifs</i>	Gifs.
<i>jpegs</i>	Jpegs.
<i>pngs</i>	Pngs.
<i>js</i>	Js.
<i>xmls</i>	Xmls.
<i>jsons</i>	Jsons.
<i>css</i>	Css.
<i>htmls</i>	Htmls.
<i>aspx</i>	Aspx.
<i>cms</i>	Cms.

Example

```
no include-url-types jpegs htmls
```

Syntax

```
geo-ip-resolution
```

Mode

AppFlow

Description

Enable geo-ip and name resolution.

Example

```
geo-ip-resolution
```

Syntax

```
no geo-ip-resolution
```

Mode

AppFlow

Description

Disable geo-ip and name resolution.

Example

```
no geo-ip-resolution
```

Syntax

```
report ipv6-flows
```

Mode

AppFlow

Description

Enable reporting IPv6 flows (all).

Example

```
report ipv6-flows
```

Syntax

```
no report ipv6-flows
```

Mode

AppFlow

Description

Disable reporting IPv6 flows (all).

Example

```
no report ipv6-flows
```

Syntax

```
gmsflow-server
```

Mode

AppFlow

Description

Enter GMS flow server configuration mode.

Example

```
gmsflow-server
```

Syntax

```
flows
```

Mode

GMSFlow Server

Description

Enable sending appflow to SonicWALL GMS flow server.

Example

```
flows
```

Syntax

```
no flows
```

Mode

GMSFlow Server

Description

Disable sending appflow to SonicWALL GMS flow server.

Example

```
no flows
```

Syntax

```
real-time
```

Mode

GMSFlow Server

Description

Enable sending of real-time data to SonicWALL GMS flow server.

Example

```
real-time
```

Syntax

```
no real-time
```

Mode

GMSFlow Server

Description

Disable sending of real-time flows to SonicWALL GMS flow server.

Example

no real-time

Syntax

system-logs

Mode

GMSFlow Server

Description

Enable sending system logs to SonicWALL GMS flow server.

Example

system-logs

Syntax

no system-logs

Mode

GMSFlow Server

Description

Disable sending system logs to SonicWALL GMS flow server.

Example

no system-logs

Syntax

report open

Mode

GMSFlow Server

Description

Enable report on connection OPEN.

Example

report open

Syntax

no report open

Mode

GMSFlow Server

Description

Disable report on connection OPEN.

Example

no report open

Syntax

```
report close
```

Mode

GMSFlow Server

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

GMSFlow Server

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

GMSFlow Server

Description

Enable report connections on the specified updates.

Options

threat	Threat detection.
application	Application detection.
user	User detection.
vpn-tunnel	VPN tunnel detection.
url	URL detection.

Example

```
report update application user
```

Syntax

```
no report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

GMSFlow Server

Description

Disable report connections on the specified updates.

Options

threat	Threat detection.
application	Application detection.
user	User detection.
vpn-tunnel	VPN tunnel detection.
url	URL detection.

Example

```
no report update application user
```

Syntax

```
reporting-format { ipfix-with-extension | ipfix-with-extension-v2 }
```

Mode

GMSFlow Server

Description

Select appflow reporting format.

Options

- ipfix-with-extension** IPFIX with extension.
- ipfix-with-extension-v2** IPFIX with extension v2.

Example

```
reporting-format ipfix-with-extension
```

Syntax

```
dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

GMSFlow Server

Description

Enable send dynamic appflow for specified tables.

Options

- connections** Connections.
- users** Users.
- urls** URLs.
- url-ratings** URL ratings.
- vpns** VPNs.
- devices** Devices.
- spams** SPAMs
- locations** Locations.
- voips** VOIPs.

Example

```
dynamic-flows connections users urls
```

Syntax

```
no dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

Description

Disable send dynamic appflow for specified tables.

Options

<i>connections</i>	Connections.
<i>users</i>	Users.
<i>urls</i>	URLs.
<i>url-ratings</i>	URL ratings.
<i>vpns</i>	VPNs.
<i>devices</i>	Devices.
<i>spams</i>	SPAMs
<i>locations</i>	Locations.
<i>voips</i>	VOIPs.

Example

```
no dynamic-flows connections users urls
```

Syntax

```
mode { advanced | basic }
```

Mode

GMSFlow Server

Description

Select GMS flow server configuration mode.

Options

<i>advanced</i>	Select advanced GMS flow server configuration mode.
<i>basic</i>	Select basic GMS flow server configuration mode.

Example

```
mode basic
```

Syntax

```
auto-synchronize
```

Mode

GMSFlow Server

Description

Enable auto-synchronize for GMS flow server.

Example

```
auto-synchronize
```

Syntax

```
no auto-synchronize
```

Mode

Description

Disable auto-synchronize for GMS flow server.

Example

```
no auto-synchronize
```

Syntax

```
advanced-mode { active-standby | load-balancing }
```

Mode

GMSFlow Server

Description

Select Advanced GMS flow server configuration mode.

Options

active-standby Select Advanced GMS flow server configuration as ActiveStandby mode.

load-balancing Select Advanced GMS flow server configuration as load-balancing mode.

Example

```
advanced-mode active-standby
```

Syntax

```
load-balancing-mode { mirror | share-load }
```

Mode

GMSFlow Server

Description

Select load balancing mode.

Options

mirror Select load balancing as mirror mode.

share-load Select load balancing as share load mode.

Example

```
load-balancing-mode share-load
```

Syntax

```
server-ip
```

Mode

GMSFlow Server

Description

Enter GMS flow server IP configuration mode.

Example

server-ip

Syntax

server ip <IPV4_HOST>

Mode

GMSFlow Server IP

Description

Set GMS flow server IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

server ip 10.10.10.200

Syntax

no server ip

Mode

GMSFlow Server IP

Description

Clear GMS flow server IP address.

Example

no server ip

Syntax

server address { { { fqdn <ADDR_FQDN> | name <ADDR_FQDNHOST_ADDR_MIXED> } | { [ipv6] host <ADDR_HOST> } } }

Mode

GMSFlow Server IP

Description

Set GMS flow server IP address.

Options

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

name Address object name.
<ADDR_FQDNHOST_ADDR_MIXED> FQDN/host address object name.
Example: *Web Server*

ipv6 IPv6.
host Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

server address name abc

Syntax

vpn-source-ip <IPv4_HOST>

Mode

GMSFlow Server IP

Description

Set source IP to use for GMS flow server on a VPN tunnel.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

vpn-source-ip 10.10.10.110

Syntax

no vpn-source-ip

Mode

GMSFlow Server IP

Description

Clear source IP to use for GMS flow server on a VPN tunnel.

Example

no vpn-source-ip

Syntax

communication-timeout <UINT8>

Mode

GMSFlow Server IP

Description

Set the GMS flow server communication timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

communication-timeout 60

Syntax

synchronize

Mode

GMSFlow Server IP

Description

Synchronize GMS flow server.

Example

synchronize

Syntax

synchronize-logs

Mode

GMSFlow Server IP

Description

Send All Log Settings GMSFlow Server.

Example

synchronize-logs

Syntax

test-connectivity

Mode

GMSFlow Server IP

Description

Test connectivity of GMS flow server.

Example

test-connectivity

Syntax

server-2-ip

Mode

GMSFlow Server

Description

Enter GMS flow server 2 IP configuration mode.

Example

server-2-ip

Syntax

server ip <IPV4_HOST>

Mode

Description

Set GMS flow server 2 IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

server ip 10.10.10.200

Syntax

no server ip

Mode

GMSFlow Server 2 IP

Description

Clear GMS flow server 2 IP address.

Example

no server ip

Syntax

server address { { { fqdn <ADDR_FQDN> | name <ADDR_FQDNHOST_ADDR_MIXED> } | { [ipv6] host <ADDR_HOST> } } }

Mode

GMSFlow Server 2 IP

Description

Set GMS flow server 2 IP address.

Options

<i>fqdn</i>	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>name</i>	Address object name.
<ADDR_FQDNHOST_ADDR_MIXED>	FQDN/host address object name. Example: <i>Web Server</i>
<i>ipv6</i>	IPv6.
<i>host</i>	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

server address name abc

Syntax

vpn-source-ip <IPV4_HOST>

Mode

GMSFlow Server 2 IP

Description

Set source IP to use for GMS flow server 2 on a VPN tunnel.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
vpn-source-ip 10.10.10.110
```

Syntax

```
no vpn-source-ip
```

Mode

GMSFlow Server 2 IP

Description

Clear source IP to use for GMS flow server 2 on a VPN tunnel.

Example

```
no vpn-source-ip
```

Syntax

```
communication-timeout <UINT8>
```

Mode

GMSFlow Server 2 IP

Description

Set the GMS flow server 2 communication timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
communication-timeout 60
```

Syntax

```
synchronize
```

Mode

GMSFlow Server 2 IP

Description

Synchronize GMS flow server 2.

Example

```
synchronize
```

Syntax

synchronize-logs

Mode

GMSFlow Server 2 IP

Description

Send All Log Settings GMSFlow Server 2.

Example

synchronize-logs

Syntax

test-connectivity

Mode

GMSFlow Server 2 IP

Description

Test connectivity of GMS flow server.

Example

test-connectivity

Syntax

sfr-mailing

Mode

AppFlow

Description

Enter SFR mailing configuration mode.

Example

sfr-mailing

Syntax

send-email

Mode

sfr Mailing

Description

Enable sending report by email.

Example

send-email

Syntax

no send-email

Mode

sfr Mailing

Description

Disable sending report by email.

Example

no send-email

Syntax

smtp-server-host <HOSTNAME_MIXED>

Mode

sfr Mailing

Description

SMTP server host name.

Options

<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

smtp-server-host 1.1.1.1
smtp-server-host mySmtpServer

Syntax

no smtp-server-host

Mode

sfr Mailing

Description

Clear SMTP server host name.

Example

no smtp-server-host

Syntax

report-to-email <EMAIL>

Mode

sfr Mailing

Description

Email address to send report on.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: support@sonicwall.com

Example

```
report-to-email abc@pqr.xyz
```

Syntax

```
no report-to-email
```

Mode

sfr Mailing

Description

Clear email address for receiving mail.

Example

```
no report-to-email
```

Syntax

```
report-from-email <EMAIL>
```

Mode

sfr Mailing

Description

Email address to send report from.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
report-from-email abc@pqr.xyz
```

Syntax

```
no report-from-email
```

Mode

sfr Mailing

Description

Clear email address for sending mail.

Example

```
no report-from-email
```

Syntax

```
smtp-server-port <IPV4_PORT>
```

Mode

sfr Mailing

Description

SMTP server port number.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
smtp-server-port 25
```

Syntax

```
security-method { ssl-tls | starttls }
```

Mode

sfr Mailing

Description

Set the connection security method.

Options

ssl-tls SSL or TLS

starttls STARTTLS

Example

```
security-method ssl-tls
```

Syntax

```
no security-method
```

Mode

sfr Mailing

Description

Set the connection security method to none.

Example

```
no security-method
```

Syntax

```
smtp-auth
```

Mode

sfr Mailing

Description

Enable SMTP authentication.

Example

```
smtp-auth
```

Syntax

```
no smtp-auth
```

Mode

sfr Mailing

Description

Disable SMTP authentication.

Example

```
no smtp-auth
```

Syntax

```
smtp-user <WORD>
```

Mode

sfr Mailing

Description

SMTP server user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
smtp-user username
```

Syntax

```
no smtp-user
```

Mode

sfr Mailing

Description

Clear SMTP server user name.

Example

```
no smtp-user
```

Syntax

```
smtp-pass <ENC_PASSWORD>
```

Mode

sfr Mailing

Description

SMTP server password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
smtp-pass *****
```

Syntax

```
no smtp-pass
```

Mode

sfr Mailing

Description

Clear SMTP server password.

Example

```
no smtp-pass
```

Syntax

```
pop-before-smtp
```

Mode

sfr Mailing

Description

Enable POP before SMTP.

Example

```
pop-before-smtp
```

Syntax

```
no pop-before-smtp
```

Mode

sfr Mailing

Description

Disable POP before SMTP.

Example

```
no pop-before-smtp
```

Syntax

```
pop-server-address <IPV4_HOST>
```

Mode

sfr Mailing

Description

POP server address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.

Example: 192.168.168.168

Example

```
pop-server-address 1.1.1.1
```

Syntax

```
no pop-server-address
```

Mode

sfr Mailing

Description

Clear POP server address.

Example

```
no pop-server-address
```

Syntax

```
pop-username <WORD>
```

Mode

sfr Mailing

Description

POP server user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
pop-username user1
```

Syntax

```
no pop-username
```

Mode

sfr Mailing

Description

Clear POP server user name.

Example

```
no pop-username
```

Syntax

```
pop-pass <ENC_PASSWORD>
```

Mode

sfr Mailing

Description

POP server password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
pop-pass *****
```

Syntax

```
no pop-pass
```

Mode

sfr Mailing

Description

Clear POP server password.

Example

```
no pop-pass
```

Syntax

```
test-email send-email smtp-server-host <HOSTNAME_MIXED> report-to-email <EMAIL> report-from-email <EMAIL> smtp-server-port <IPV4_PORT> security-method { none | ssl-tls | starttls } [ smtp-auth ] [ smtp-user <WORD> ] [ smtp-pass <WORD> ] [ pop-before-smtp ] [ pop-server-address <IPV4_HOST> ] [ pop-username <WORD> ] [ pop-pass <WORD> ]
```

Mode

sfr Mailing

Description

Test SFR email settings.

Options

send-email	Enable sending report by email.
smtp-server-host	SMTP server host name.
<HOSTNAME_MIXED>	IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
report-to-email	Email address to send report on.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
report-from-email	Email address to send report from.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
smtp-server-port	SMTP server port number.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
security-method	Set the connection security method.
none	SSL or TLS
ssl-tls	SSL or TLS
starttls	STARTTLS
smtp-auth	Enable SMTP authentication.
smtp-user	SMTP server user name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
smtp-pass	SMTP server password.

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
pop-before-smtp	Enable POP before SMTP.
pop-server-address	POP server address.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
pop-username	POP server user name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
pop-pass	POP server password.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

test-email

Syntax

appflow-server

Mode

AppFlow

Description

Enter appflow server configuration mode.

Example

appflow-server

Syntax

flows

Mode

AppFlow Server

Description

Enable sending appflow to SonicWALL appflow server.

Example

flows

Syntax

no flows

Mode

AppFlow Server

Description

Disable sending appflow to SonicWALL appflow server.

Example

no flows

Syntax

real-time

Mode

AppFlow Server

Description

Enable sending of real-time data to SonicWALL appflow server.

Example

real-time

Syntax

no real-time

Mode

AppFlow Server

Description

Disable sending of real-time data to SonicWALL appflow server.

Example

no real-time

Syntax

system-logs

Mode

AppFlow Server

Description

Enable sending of system log to SonicWALL appflow server.

Example

system-logs

Syntax

no system-logs

Mode

AppFlow Server

Description

Disable sending of system log to SonicWALL appflow server.

Example

no system-logs

Syntax

report open

Mode

AppFlow Server

Description

Enable report on connection OPEN.

Example

```
report open
```

Syntax

```
no report open
```

Mode

AppFlow Server

Description

Disable report on connection OPEN.

Example

```
no report open
```

Syntax

```
report close
```

Mode

AppFlow Server

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

AppFlow Server

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

AppFlow Server

Description

Enable report connections on the specified updates.

Options

<i>threat</i>	Threat detection.
<i>application</i>	Application detection.
<i>user</i>	User detection.
<i>vpn-tunnel</i>	VPN tunnel detection.
<i>url</i>	URL detection.

Example

```
report update application user
```

Syntax

```
no report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

AppFlow Server

Description

Disable report connections on the specified updates.

Options

<i>threat</i>	Threat detection.
<i>application</i>	Application detection.
<i>user</i>	User detection.
<i>vpn-tunnel</i>	VPN tunnel detection.
<i>url</i>	URL detection.

Example

```
no report update application user
```

Syntax

```
dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

AppFlow Server

Description

Enable send dynamic appflow for specified tables.

Options

<i>connections</i>	Connections.
<i>users</i>	Users.
<i>urls</i>	URLs.
<i>url-ratings</i>	URL ratings.
<i>vpns</i>	VPNs.
<i>devices</i>	Devices.
<i>spams</i>	SPAMs
<i>locations</i>	Locations.
<i>voips</i>	VOIPs.

Example

```
dynamic-flows connections users urls
```

Syntax

```
no dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

AppFlow Server

Description

Disable send dynamic appflow for specified tables.

Options

<i>connections</i>	Connections.
<i>users</i>	Users.
<i>urls</i>	URLs.
<i>url-ratings</i>	URL ratings.
<i>vpns</i>	VPNs.
<i>devices</i>	Devices.
<i>spams</i>	SPAMs
<i>locations</i>	Locations.
<i>voips</i>	VOIPs.

Example

```
no dynamic-flows connections users urls
```

Syntax

```
keep-alive
```

Mode

AppFlow Server

Description

Enable keep-alive with appflow server.

Example

```
keep-alive
```

Syntax

```
no keep-alive
```

Mode

AppFlow Server

Description

Disable keep-alive with appflow server.

Example

```
no keep-alive
```

Syntax

```
mode { advanced | basic }
```

Mode

AppFlow Server

Description

Select APP flow server configuration mode.

Options

advanced Select advanced APP flow server configuration mode.

basic Select basic APP flow server configuration mode.

Example

```
mode basic
```

Syntax

```
auto-synchronize
```

Mode

AppFlow Server

Description

Enable auto-synchronize for appflow server.

Example

```
auto-synchronize
```

Syntax

```
no auto-synchronize
```

Mode

AppFlow Server

Description

Disable auto-synchronize for appflow server.

Example

```
no auto-synchronize
```

Syntax

```
advanced-mode { active-standby | load-balancing }
```

Mode

AppFlow Server

Description

Select Advanced APP flow server configuration mode.

Options

active-standby Select Advanced APP flow server configuration as ActiveStandby mode.

load-balancing Select Advanced APP flow server configuration as load-balancing mode.

Example

advanced-mode active-standby

Syntax

load-balancing-mode { mirror | share-load }

Mode

AppFlow Server

Description

Select load balancing mode.

Options

mirror Select load balancing as mirror mode.

share-load Select load balancing as share load mode.

Example

load-balancing-mode share-load

Syntax

server-ip

Mode

AppFlow Server

Description

Enter appflow server IP configuration mode.

Example

server-ip

Syntax

server ip <IPV4_HOST>

Mode

AppFlow Server IP

Description

Set App flow server IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

server ip 10.10.10.200

Syntax

no server ip

Mode

AppFlow Server IP

Description

Clear App flow server IP address.

Example

no server ip

Syntax

server address { { { fqdn <ADDR_FQDN> | name <ADDR_FQDNHOST_ADDR_MIXED> } | { [ipv6] host <ADDR_HOST> } } }

Mode

AppFlow Server IP

Description

Set App flow server IP address.

Options

fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
name <ADDR_FQDNHOST_ADDR_MIXED>	Address object name. FQDN/host address object name. Example: <i>Web Server</i>
ipv6 host <ADDR_HOST>	IPv6. Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

server address name abc

Syntax

vpn-source-ip <IPV4_HOST>

Mode

AppFlow Server IP

Description

Set source IP to use for appflow server on a VPN tunnel.

Options

<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

vpn-source-ip 10.10.10.110

Syntax

```
no vpn-source-ip
```

Mode

AppFlow Server IP

Description

Clear source IP to use for appflow server on a VPN tunnel.

Example

```
no vpn-source-ip
```

Syntax

```
max-flows <UINT32>
```

Mode

AppFlow Server IP

Description

Set the appflow server maximum flows.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
max-flows 500000
```

Syntax

```
communication-timeout <UINT8>
```

Mode

AppFlow Server IP

Description

Set the appflow server communication timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
communication-timeout 60
```

Syntax

```
firewall-name <WORD>
```

Mode

AppFlow Server IP

Description

Set the appflow server firewall name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
firewall-name "My Sonicwall"
```

Syntax

```
passphrase <ENC_PASSWORD>
```

Mode

AppFlow Server IP

Description

Set the connection passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
passphrase reveal2noone
```

Syntax

```
no passphrase
```

Mode

AppFlow Server IP

Description

Clear the connection passphrase.

Example

```
no passphrase
```

Syntax

```
synchronize
```

Mode

AppFlow Server IP

Description

Synchronize appflow server.

Example

```
synchronize
```

Syntax

```
synchronize-logs
```

Mode

AppFlow Server IP

Description

Synchronize log settings.

Example

```
synchronize-logs
```

Syntax

```
test-connectivity
```

Mode

AppFlow Server IP

Description

Test connectivity of appflow server.

Example

```
test-connectivity
```

Syntax

```
flush server <IPV4_HOST>
```

Mode

AppFlow Server

Description

Flush specified appflow server.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
flush server 192.168.168.166
```

Syntax

```
flush servers
```

Mode

AppFlow Server

Description

Flush all discovered appflow servers.

Example

```
flush servers
```

Syntax

```
discover <ASSIGNED_INTERFACE>
```


Mode

AppFlow Server

Description

Discover appflow servers.

Options

<ASSIGNED_INTERFACE> Interface name.
Example: *X0*

Example

```
discover interfaceId
```

Syntax

```
server-2-ip
```

Mode

AppFlow Server

Description

Enter appflow server 2 IP configuration mode.

Example

```
server-2-ip
```

Syntax

```
server ip <IPV4_HOST>
```

Mode

AppFlow Server 2 IP

Description

Set App flow server 2 IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
server ip 10.10.10.200
```

Syntax

```
no server ip
```

Mode

AppFlow Server 2 IP

Description

Clear App flow server 2 IP address.

Example

```
no server ip
```

Syntax

```
server address { { { fqdn <ADDR_FQDN> | name <ADDR_FQDNHOST_ADDR_MIXED> } | { [ ipv6 ] host <ADDR_HOST> } } }
```

Mode

AppFlow Server 2 IP

Description

Set App flow server 2 IP address.

Options

<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>name</i> <ADDR_FQDNHOST_ADDR_MIXED>	Address object name. FQDN/host address object name. Example: <i>Web Server</i>
<i>ipv6</i> <i>host</i> <ADDR_HOST>	IPv6. Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

```
server address name abc
```

Syntax

```
vpn-source-ip <IPV4_HOST>
```

Mode

AppFlow Server 2 IP

Description

Set source IP to use for appflow server 2 on a VPN tunnel.

Options

<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
vpn-source-ip 10.10.10.110
```

Syntax

```
no vpn-source-ip
```

Mode

AppFlow Server 2 IP

Description

Clear source IP to use for appflow server 2 on a VPN tunnel.

Example

no vpn-source-ip

Syntax

max-flows <UINT32>

Mode

AppFlow Server 2 IP

Description

Set the appflow server 2 maximum flows.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

max-flows 500000

Syntax

communication-timeout <UINT8>

Mode

AppFlow Server 2 IP

Description

Set the appflow server 2 communication timeout in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

communication-timeout 60

Syntax

firewall-name <WORD>

Mode

AppFlow Server 2 IP

Description

Set the appflow server 2 firewall name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

firewall-name "My Sonicwall"

Syntax

passphrase <ENC_PASSWORD>

Mode

AppFlow Server 2 IP

Description

Set the connection passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

passphrase reveal2noone

Syntax

no passphrase

Mode

AppFlow Server 2 IP

Description

Clear the connection passphrase.

Example

no passphrase

Syntax

synchronize

Mode

AppFlow Server 2 IP

Description

Synchronize appflow server 2.

Example

synchronize

Syntax

synchronize-logs

Mode

AppFlow Server 2 IP

Description

Synchronize log settings.

Example

synchronize-logs

Syntax

test-connectivity

Mode

AppFlow Server 2 IP

Description

Test connectivity of appflow server.

Example

test-connectivity

Syntax

external-collector

Mode

AppFlow

Description

Enter external collector configuration mode.

Example

external-collector

Syntax

flows

Mode

External Collector

Description

Enable sending appflow and real-time data to external collector.

Example

flows

Syntax

no flows

Mode

External Collector

Description

Disable sending appflow and real-time data to external collector.

Example

no flows

Syntax

reporting-format { ipfix | ipfix-with-extensions | netflow-5 | netflow-9 }

Mode

External Collector

Description

Set the external appflow reporting format.

Options

<i>ipfix</i>	IPFIX.
<i>ipfix-with-extensions</i>	IPFIX with extensions.
<i>netflow-5</i>	Netflow version 5.
<i>netflow-9</i>	Netflow version 9.

Example

```
reporting-format ipfix
```

Syntax

```
no server ip
```

Mode

External Collector

Description

Clear external collector IP address.

Example

```
no server ip
```

Syntax

```
server ip <IPV4_HOST>
```

Mode

External Collector

Description

Set external collector IP address.

Options

<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168

Example

```
server ip 10.10.10.200
```

Syntax

```
server address { { { fqdn <ADDR_FQDN> | name <ADDR_FQDNHOST_ADDR_MIXED> } | { [ ipv6 ] host <ADDR_HOST> } } }
```

Mode

External Collector

Description

Set external collector IP address.

Options

<i>fqdn</i>	Address object full qualified domain name.
<i><ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>name</i>	Address object name.
<i><ADDR_FQDNHOST_ADDR_MIXED></i>	FQDN/host address object name. Example: <i>Web Server</i>
<i>ipv6</i>	IPv6.
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

server ip 10.10.10.200

Syntax

vpn-source-ip <IPv4_HOST>

Mode

External Collector

Description

Set source IP to use for external collector on a VPN tunnel.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

vpn-source-ip 10.10.10.110

Syntax

no vpn-source-ip

Mode

External Collector

Description

Clear source IP to use for external collector on a VPN tunnel.

Example

no vpn-source-ip

Syntax

port <UINT16>

Mode

External Collector

Description

Set external collector UDP port number.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
port 2055
```

Syntax

```
send templates
```

Mode

External Collector

Description

Enable sending of netflow/ipfix templates at regular intervals.

Example

```
send templates
```

Syntax

```
no send templates
```

Mode

External Collector

Description

Disable sending of netflow/ipfix templates at regular intervals.

Example

```
no send templates
```

Syntax

```
send static-flows
```

Mode

External Collector

Description

Enable sending of static appflow at regular intervals.

Example

```
send static-flows
```

Syntax

```
no send static-flows
```


Mode

External Collector

Description

Disable sending of static appflow at regular intervals.

Example

```
no send static-flows
```

Syntax

```
static-flows { [ applications ] [ viruses ] [ spyware ] [ intrusions ] [ location-map ] [ services ] [ rating-map ] [ table-map ] [ column-map ] }
```

Mode

External Collector

Description

Enable tables to send static appflows for.

Options

applications	Applications.
viruses	Viruses.
spyware	Spyware.
intrusions	Intrusions.
location-map	Location map.
services	Services.
rating-map	Rating map.
table-map	Table map.
column-map	Column map.

Example

```
static-flows applications spyware
```

Syntax

```
no static-flows { [ applications ] [ viruses ] [ spyware ] [ intrusions ] [ location-map ] [ services ] [ rating-map ] [ table-map ] [ column-map ] }
```

Mode

External Collector

Description

Disable tables to send static appflows for.

Options

applications	Applications.
viruses	Viruses.
spyware	Spyware.
intrusions	Intrusions.
location-map	Location map.
services	Services.
rating-map	Rating map.
table-map	Table map.
column-map	Column map.

Example

```
no static-flows applications spyware
```

Syntax

```
dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

External Collector

Description

Enable tables to send dynamic appflows for.

Options

connections	Connections.
users	Users.
urls	URLs.
url-ratings	URL ratings.
vpns	VPNs.
devices	Devices.
spams	SPAMs
locations	Locations.
voips	VOIPs.

Example

```
dynamic-flows applications spyware
```

Syntax

```
no dynamic-flows { [ connections ] [ users ] [ urls ] [ url-ratings ] [ vpns ] [ devices ] [ spams ] [ locations ] [ voips ] }
```

Mode

External Collector

Description

Disable tables to send dynamic appflows for.

Options

connections	Connections.
users	Users.
urls	URLs.
url-ratings	URL ratings.
vpns	VPNs.
devices	Devices.
spams	SPAMs
locations	Locations.
voips	VOIPs.

Example

```
no dynamic-flows applications spyware
```

Syntax

```
ipfix-reports { [ top-10-apps ] [ interface-statistics ] [ core-utilization ] [ memory-utilization ] [ system-logs ] [ sdwan-probe ] }
```

Mode

External Collector

Description

Enable including of specified additional reports via IPFIX.

Options

<i>top-10-apps</i>	Top 10 applications.
<i>interface-statistics</i>	Interface statistics.
<i>core-utilization</i>	Core utilization.
<i>memory-utilization</i>	Memory utilization.
<i>system-logs</i>	System logs.
<i>sdwan-probe</i>	SD-WAN probe stats.

Example

```
ipfix-reports top-10-apps memory-utilization
```

Syntax

```
no ipfix-reports { [ top-10-apps ] [ interface-statistics ] [ core-utilization ] [ memory-utilization ] [ system-logs ] [ sdwan-probe ] }
```

Mode

External Collector

Description

Disable including of specified additional reports via IPFIX.

Options

<i>top-10-apps</i>	Top 10 applications.
<i>interface-statistics</i>	Interface statistics.
<i>core-utilization</i>	Core utilization.
<i>memory-utilization</i>	Memory utilization.
<i>system-logs</i>	System logs.
<i>sdwan-probe</i>	SD-WAN probe stats.

Example

```
no ipfix-reports top-10-apps memory-utilization
```

Syntax

```
report open
```

Mode

External Collector

Description

Enable report on connection OPEN.

Example

```
report open
```

Syntax

```
no report open
```

Mode

External Collector

Description

Disable report on connection OPEN.

Example

```
no report open
```

Syntax

```
report close
```

Mode

External Collector

Description

Enable report on connection CLOSE.

Example

```
report close
```

Syntax

```
no report close
```

Mode

External Collector

Description

Disable report on connection CLOSE.

Example

```
no report close
```

Syntax

```
report active-timeout <UINT8>
```

Mode

External Collector

Description

Enable report connection on active timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
report active-timeout 60
```

Syntax

```
no report active-timeout
```

Mode

External Collector

Description

Disable report connection on active timeout.

Example

```
no report active-timeout
```

Syntax

```
report kilobytes-exchanged [ kilobytes <UINT16> ] [ once ]
```

Mode

External Collector

Description

Enable report connection on kilobytes exchanged.

Options

kilobytes Specify kilobytes.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*
once Report once.

Example

```
report kilobytes-exchanged kilobytes 100
report kilobytes-exchanged
report kilobytes-exchanged kilobytes 200 once
```

Syntax

```
no report kilobytes-exchanged [ once ]
```

Mode

External Collector

Description

Disable report connection on kilobytes exchanged.

Options

once Report once.

Example

```
no report kilobytes-exchanged
```

Syntax

```
report update { [ threat ] [ application ] [ user ] [ vpn-tunnel ] [ url ] }
```

Mode

External Collector

Description

Enable report connections on the specified updates.

Options

threat Threat detection.
application Application detection.
user User detection.
vpn-tunnel VPN tunnel detection.

url URL detection.

Example

report update application user

Syntax

no report update { [threat] [application] [user] [vpn-tunnel] [url] }

Mode

External Collector

Description

Disable report connections on the specified updates.

Options

- threat** Threat detection.
- application** Application detection.
- user** User detection.
- vpn-tunnel** VPN tunnel detection.
- url** URL detection.

Example

no report update application user

Syntax

generate all-templates

Mode

External Collector

Description

Generate all templates.

Example

generate all-templates

Syntax

generate static-appflow-data

Mode

External Collector

Description

Generate static appflow data.

Example

generate static-appflow-data

Syntax

send-all-entries

Mode

External Collector

Description

Send the necessary fields of log settings to external collector for log display.

Example

send-all-entries

Syntax

```
cta-report [ locale <WORD> ] [ style <WORD> ] [ snce <UINT8> ] [ report <WORD> ] [ txt <WORD> ] [ comp-name <WORD> ] [ prpr-name <WORD> ] [ phn <WORD> ] [ mail <WORD> ] [ exec-only <UINT8> ] [ app-hlts <UINT8> ] [ thrts <UINT8> ] [ btnt <UINT8> ] [ usr-sesn <UINT8> ] [ rsk-app <UINT8> ] [ mlwr <UINT8> ] [ cntr-trfc <UINT8> ] [ usr-trfc <UINT8> ] [ wb-act <UINT8> ] [ explts <UINT8> ] [ ip-sesn <UINT8> ] [ rprr-cnf <UINT8> ] [ fle-trnsfr <UINT8> ] [ kn-unk-mlwr <UINT8> ] [ ip-trafc <UINT8> ] [ logo <WORD> ]
```

Mode

Config

Description

Exporting CTA report.

Options

locale <WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
style <WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
snce <UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
report <WORD>	Report title Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
txt <WORD>	About text Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
comp-name <WORD>	Company name Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
prpr-name <WORD>	Preparer name Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
phn <WORD>	phone contact Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
mail <WORD>	Email contact Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
exec-only <UINT8>	Executive summary only Integer in the form: D OR 0xHH. Example: <i>123</i>
app-hlts <UINT8>	Application highlights Integer in the form: D OR 0xHH. Example: <i>123</i>
thrts <UINT8>	Glimpse of the threats Integer in the form: D OR 0xHH. Example: <i>123</i>
btnt <UINT8>	Botnet analysis Integer in the form: D OR 0xHH. Example: <i>123</i>
usr-sesn <UINT8>	Top users by sessions Integer in the form: D OR 0xHH. Example: <i>123</i>
rsk-app	Risk Applications

<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
mlwr	Malware analysis
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
cntr-trfc	Top countries by traffic
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
usr-trfc	Top users by traffic
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
wb-act	Web activity
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
expls	Exploits Used
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
ip-sesn	Top IPs by sessions
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
rprr-cnf	Report configuration
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
fle-trnsfr	File transfer investigation
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
kn-unk-mlwr	Known and unknown malware
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
ip-trafc	Top IPs by traffic
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
logo	Top IPs by traffic
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Syntax

```
no cta-report <UINT64>
```

Mode

Config

Description

Delete generated CTA report.

Options

<UINT64>	Integer in the form: D OR 0xHHHHHHHHHHHHHHHHHH. Example: <i>123</i>

Example

```
no cta-report 1594896359528
```

Syntax

```
reset appflow-report
```

Mode

Config

Description

Reset appflow report.

Example

reset appflow-report

Syntax

```
show appflow [ [ appflow-server | base | external-collector | gmsflow-server | sfr-mailing ] [ { pending-config | with-pending-config } ] | statistics [ { external | internal | ipfix } ] | status [ { appflow-server | gmsflow-server } ] ]
```

Mode

All Modes

Description

Show appflow configuration.

Options

<i>appflow-server</i>	Show appflow server configuration.
<i>base</i>	Show appflow base configuration.
<i>external-collector</i>	Show external collector configuration.
<i>gmsflow-server</i>	Show GMS flow server configuration.
<i>sfr-mailing</i>	Show appflow SFR-mailing configuration.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show appflow statistics.
<i>external</i>	Show external flow reporting statistics.
<i>internal</i>	Show internal appflow reporting statistics.
<i>ipfix</i>	Show total IPFIX statistics.
<i>status</i>	Show appflow status.
<i>appflow-server</i>	Show appflow server status.
<i>gmsflow-server</i>	Show GMS flow server status.

Example

```
show appflow
```

Syntax

```
certificates
```

Mode

Config

Description

Certificate configuration.

Example

```
certificates
```

Syntax

```
export signing-request <CERT_NAME> { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Certificates

Description

Export certificate signing request.

Options

<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export signing-request "Corp VPN Cert" ftp ftp://ftp.myserver.local/cert.p10
export signing-request "Corp VPN Cert" scp user@server:/home/user/cert.p10
export signing-request "Corp VPN Cert" scp user@server:/home/user/
```

Syntax

```
export cert-key-pair <CERT_NAME> password <WORD> { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Certificates

Description

Export certificate signing request or certificate / key pair.

Options

<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
password	Password of the PKCS#12 (.p12 or .pfx) encoded file.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export cert-key-pair "Corp VPN Cert" password pwd ftp ftp://ftp.myserver.local/cert.p12
export cert-key-pair "Corp VPN Cert" password pwd scp user@server:/home/user/cert.p12
export cert-key-pair "Corp VPN Cert" password pwd scp user@server:/home/user/
```

Syntax

```
import cert-key-pair <WORD> password <WORD> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Certificates

Description

Import certificate / key pair.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
password	Password of the PKCS#12 (.p12 or .pfx) encoded file.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import cert-key-pair "Corp VPN Cert" password pwd ftp ftp://ftp.myserver.local/cert.p12
import cert-key-pair "Corp VPN Cert" password pwd scp user@server:/home/user/cert.p12
```

Syntax

```
import ca-cert { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Certificates

Description

Import CA certificate.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import ca-cert ftp ftp://ftp.myserver.local/cacert.crt
import ca-cert scp user@server:/home/user/cacert.crt
```

Syntax

```
import signed-cert <CERT_NAME> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Certificates

Description

Import CA signed certificate.

Options

<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import signed-cert "Corp VPN Cert" ftp ftp://ftp.myserver.local/cert.crt
import signed-cert "Corp VPN Cert" scp user@server:/home/user/cert.crt
```

Syntax

```
import crl ca-name <CERT_NAME> { [ disable-invalidate-certificates | invalidate-certificates ] [ directly { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] } | periodically <WEB_URL> ] }
```

Mode

Certificates

Description

Import certificate revocation list or set the location to periodically download via HTTP.

Options

ca-name	CA certificate associated with CRL.
<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
disable-invalidate-certificates	Disable invalidate certificates and security associations if CRL import or processing fails.
invalidate-certificates	Invalidate certificates and security associations if CRL import or processing fails.
directly	Import CRL directly from a PEM (.pem) or DER (.der or .crl) encoded file.
api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

<i>periodically</i>	Periodically auto-import CRL via HTTP.
<i><WEB_URL></i>	URL in the form: <code>http://host/file</code> . Example: <code>http://www.example.com/products/</code>

Example

```
import crl ca-name "Corp CA Cert" directly ftp ftp://ftp.myserver.local/cert.crl
import crl ca-name "Corp CA Cert" invalidate-certificates
```

Syntax

```
no certificate <CERT_NAME>
```

Mode

Certificates

Description

Delete signing request or certificate / key pair.

Options

<CERT_NAME> Certificate name.
Example: `my_cert`

Example

```
no certificate "Corp VPN Cert"
```

Syntax

```
no ca-certificate <CA_CERT_HASH>
```

Mode

Certificates

Description

Delete CA certificate.

Options

<CA_CERT_HASH> CA Certificate hash.
Example: `rBMtDf8pTii9doixKqNtcw==`

Example

```
no certificate rBMtDf8pTii9doixKqNtcw==
```

Syntax

```
no certificates
```

Mode

Certificates

Description

Delete all imported CA certificates, signing requests or certificate / key pairs.

Example

```
no certificates
```

Syntax

generate-signing-request

Mode

Certificates

Description

Enter certificate signing request configuration mode.

Example

generate-signing-request

Syntax

no enrollment

Mode

Certificates

Description

Stop enrollment for signing request.

Example

no enrollment

Syntax

scep

Mode

Certificates

Description

Enter simple certificate enrollment protocol configuration mode.

Example

scep

Syntax

alias <WORD>

Mode

Signing Request

Description

Configure certificate signing request alias.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

alias "MyCertAlias"

Syntax

distinguished-name element1 { country <CERT_COUNTRY> | locality <WORD> | organization <WORD> | state <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

- country** Country. Adds C=country-name to distinguished name.
<CERT_COUNTRY> Certificate signing request country.
Example: *afghanistan*
- locality** Locality, City, or County. Adds L=locality-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- organization** Company or organization. Adds O=orgainization-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- state** State. Adds ST=state-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

distinguished-name element1 country US

Syntax

distinguished-name element2 { country <CERT_COUNTRY> | department <WORD> | locality <WORD> | organization <WORD> | state <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

- country** Country. Adds C=country-name to distinguished name.
<CERT_COUNTRY> Certificate signing request country.
Example: *afghanistan*
- department** Department. Adds OU=department-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- locality** Locality, City, or County. Adds L=locality-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- organization** Company or organization. Adds O=orgainization-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- state** State. Adds ST=state-name to distinguished name.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

Syntax

distinguished-name element3 { department <WORD> | group <WORD> | locality <WORD> | organization <WORD> | team <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

department <WORD>	Department. Adds OU=department-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
group <WORD>	Group. Adds OU=group-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
locality <WORD>	Locality, City, or County. Adds L=locality-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
organization <WORD>	Company or organization. Adds O=orgainization-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
team <WORD>	Team. Adds OU=team-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

distinguished-name element3 locality "San Jose"

Syntax

distinguished-name element4 { common-name <WORD> | department <WORD> | email <WORD> | group <WORD> | organization <WORD> | serial <WORD> | team <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name <WORD>	Common Name. Adds CN=common-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
department <WORD>	Department. Adds OU=department-name to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
email <WORD>	E-mail Address. Adds Email=email-address to distinguished name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

group	Group. Adds OU=group-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
organization	Company or organization. Adds O=orgainization-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
serial	Serial Number. Adds SN=serial-number to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
team	Team. Adds OU=team-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

distinguished-name element4 organization "My company"

Syntax

distinguished-name element5 { common-name <WORD> | department <WORD> | email <WORD> | group <WORD> | serial <WORD> | team <WORD> }

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

common-name	Common Name. Adds CN=common-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
department	Department. Adds OU=department-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
email	E-mail Address. Adds Email=email-address to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
group	Group. Adds OU=group-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
serial	Serial Number. Adds SN=serial-number to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
team	Team. Adds OU=team-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

distinguished-name element5 department "Department"

Syntax

distinguished-name element6 { common-name <WORD> | email <WORD> | group <WORD> | serial <WORD> | team <WORD> }

Mode

Description

Configure certificate signing request distinguished name.

Options

<i>common-name</i>	Common Name. Adds CN=common-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>email</i>	E-mail Address. Adds Email=email-address to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>group</i>	Group. Adds OU=group-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>serial</i>	Serial Number. Adds SN=serial-number to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>team</i>	Team. Adds OU=team-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

distinguished-name element6 group "Group"

Syntax

distinguished-name element7 { common-name <WORD> | email <WORD> | serial <WORD> | team <WORD> }

Mode

Description

Configure certificate signing request distinguished name.

Options

<i>common-name</i>	Common Name. Adds CN=common-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>email</i>	E-mail Address. Adds Email=email-address to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>serial</i>	Serial Number. Adds SN=serial-number to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>team</i>	Team. Adds OU=team-name to distinguished name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

distinguished-name element7 team "Team"

Syntax

```
distinguished-name element8 { common-name <WORD> | email <WORD> | serial <WORD> }
```

Mode

Signing Request

Description

Configure certificate signing request distinguished name.

Options

<i>common-name</i>	Common Name. Adds CN=common-name to distinguished name.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>email</i>	E-mail Address. Adds Email=email-address to distinguished name.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>serial</i>	Serial Number. Adds SN=serial-number to distinguished name.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
distinguished-name element8 email admin@mycompany.local
```

Syntax

```
alternate-name { domain-name <HOSTNAME> | email-address <EMAIL> | ipv4-address <IPV4_HOST> }
```

Mode

Signing Request

Description

Configure certificate signing request alternate name.

Options

<i>domain-name</i>	Domain name.
<i><HOSTNAME></i>	Hostname in the form: hostname OR a.b.c.d. Example: <i>example.com</i>
<i>email-address</i>	E-mail address.
<i><EMAIL></i>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
<i>ipv4-address</i>	IP address.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
alternate-name ipv4-address 10.10.10.10
```

Syntax

```
signature-algorithm { md5 | sha-1 | sha-256 | sha-384 | sha-512 }
```

Mode

Signing Request

Description

Configure certificate signing request signature algorithm.

Options

md5 MD5.

sha-1 SHA1.

sha-256 SHA256.

sha-384 SHA384.

sha-512 SHA512.

Example

```
signature-algorithm sha-1
```

Syntax

```
key type { ecdsa | rsa }
```

Mode

Signing Request

Description

Configure certificate signing request subject key type.

Options

ecdsa ECDSA.

rsa RSA.

Example

```
key type rsa
```

Syntax

```
key size { 1024 | 1536 | 2048 | 256 | 384 | 4096 | 521 }
```

Mode

Signing Request

Description

Configure certificate signing request subject key size.

Options

1024 1024 bits.

1536 1536 bits.

2048 2048 bits.

256 prime256v1: X9.62/SECG curve over a 256 bit prime field.

384 secp384r1: NIST/SECG curve over a 384 bit prime field.

4096 4096 bits.

521 secp521r1: NIST/SECG curve over a 521 bit prime field.

Example

```
key size rsa 1024
```

Syntax

```
generate
```

Mode

Signing Request

Description

Generate certificate signing request.

Example

```
generate
```

Syntax

```
signing-request <CERT_NAME>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol signing request.

Options

<CERT_NAME> Certificate name.
Example: *my_cert*

Example

```
signing-request srlocal
```

Syntax

```
ca-url <WEB_URL>
```

Mode

SCEP

Description

Configure simple certificate enrollment protocol certificate authority URL.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
ca-url http://scep.mydomain.local
```

Syntax

challenge-password <WORD>

Mode

SCEP

Description

Configure simple certificate enrollment protocol certificate authority challenge password.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

challenge-password secret

Syntax

request-count <UINT16>

Mode

SCEP

Description

Configure simple certificate enrollment protocol request count.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

request-count 256

Syntax

polling-interval <UINT16>

Mode

SCEP

Description

Configure simple certificate enrollment protocol polling interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

polling-interval 30

Syntax

max-polling-time <UINT16>

Mode

SCEP

Description

Configure simple certificate enrollment protocol max polling time.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

max-polling-time 28800

Syntax

scep

Mode

SCEP

Description

Enable simple certificate enrollment protocol.

Example

scep

Syntax

show certificates status [build-in [with-expired] | imported]

Mode

All Modes

Description

Show certificates status.

Options

- status** Show certificates status.
- build-in** Show build in certificates.
- with-expired** Include expired build in certificates.
- imported** Show imported certificates.

Example

show certificates status

Syntax

show certificate name <CERT_NAME> status

Mode

All Modes

Description

Show certificate status.

Options

<i>name</i>	Certificate name.
<i><CERT_NAME></i>	Certificate name. Example: <i>my_cert</i>
<i>status</i>	Show certificate status.

Example

show certificate name EchoCERT status

Syntax

export log { csv | txt } { api | ftp <FTP_URL> | scp <SCP_URL> [port <IPV4_PORT>] }

Mode

Top Level
Config

Description

Export log in csv or txt format.

Options

<i>csv</i>	CSV format.
<i>txt</i>	Text format.
<i>api</i>	Export using the api.
<i>ftp</i>	Export using the FTP protocol.
<i><FTP_URL></i>	FTP URL in the form: ftp://username:password@hostname\n Escape character: ':' -> '\\:','@' -> '\\@',' ' -> '\\ ','\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
<i>scp</i>	Export using the SCP protocol.
<i><SCP_URL></i>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
<i>port</i>	SCP server port
<i><IPV4_PORT></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

export log csv ftp ftp://user:password@servername/log.csv
export log csv user@server:/home/user/log.csv
export log csv scp user@server:/home/user/

Syntax

clear log

Mode

All Modes
Top Level

Description

Clear all log entries.

Example

clear log

Syntax

log-action email

Mode

Top Level
Config

Description

Send log to configured e-mail address.

Example

```
log-action email
```

Syntax

```
log display { max-number <UINT32> | time-range { all | last <UINT8> { days | hours | minutes } } }
```

Mode

Config

Description

Configure time range and max number for showing log view in CLI.

Options

max-number Max number
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

time-range Time range.

all All entries.

last Last time range.
<UINT8> Integer in the form: D OR 0xHH.
Example: 123

days Days.

hours Hours.

minutes Minutes.

Example

```
log display max-number 100  
log display time-range last 5 minutes
```

Syntax

```
log event id <LOG_EVENT_ID>
```

Mode

Config

Description

Enter log event configuration mode with specified event ID.

Options

id Configure a event which has the specified ID.
<LOG_EVENT_ID> Event id.
Example: 200

Example

```
log event id 440
```

Syntax

```
log group id <LOG_GROUP_ID>
```

Mode

Config

Description

Enter log group configuration mode with specified group ID.

Options

id	Configure a group which has the specified ID.
<LOG_GROUP_ID>	Group id. Example: <i>20</i>

Example

```
log group id 440
```

Syntax

```
log category <LOG_CATEGORY_NAME> [ group <LOG_GROUP_NAME> [ event <LOG_EVENT_NAME> ] ]
```

Mode

Config

Description

Enter log category configuration mode.

Options

<LOG_CATEGORY_NAME>	Log category name. Example: <i>Firewall</i>
group	Group configuration.
<LOG_GROUP_NAME>	Group name. Example: <i>Firewall Event</i>
event	Event configuration.
<LOG_EVENT_NAME>	Event name. Example: <i>Activate Firewall</i>

Example

```
log category VPN
log category "Admin System" group GMS
log category Firewall group "Firewall Rule" event "Firewall Add"
```

Syntax

```
log categories
```

Mode

Config

Description

Enter log categories configuration mode.

Example

```
log categories
```

Syntax

log syslog

Mode

Config

Description

Enter syslog configuration mode.

Example

log syslog

Syntax

log automation

Mode

Config

Description

Enter log automation configuration mode.

Example

log automation

Syntax

log name-resolution

Mode

Config

Description

Enter log name resolution configuration mode.

Example

log name-resolution

Syntax

log reports

Mode

Config

Description

Enter log reports configuration mode.

Example

log reports

Syntax

```
log viewpoint
```

Mode

Config

Description

Enter viewpoint configuration mode.

Example

```
log viewpoint
```

Syntax

```
log analyzer
```

Mode

Config

Description

Enter analyzer configuration mode.

Example

```
log analyzer
```

Syntax

```
save-template <WORD>
```

Mode

Log Categories

Description

Save current log event settings in custom template.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
save-template "Current event log company specific default settings"
```

Syntax

```
import-template { analyzer-viewpoint-gms | custom | default | firewall-action | minimal }
```

Mode

Log Categories

Description

Set log event settings to what is specified in the template.

Options

analyzer-viewpoint-gms Set event log settings to work well with analyzer / viewpoint / GMS server.

custom	Set event log settings to previously saved settings.
default	Restore all event log settings to default values.
firewall-action	Set event log settings to work with firewall action template.
minimal	Set event log settings so that a minimal amount of logs are created.

Example

```
import-template default
```

Syntax

```
reset event-count { all | category <LOG_CATEGORY_NAME> [ group <LOG_GROUP_NAME> [ event <LOG_EVENT_NAME> ] ] | event-id <LOG_EVENT_ID> }
```

Mode

Log Categories

Description

Reset the event counters for specified category.

Options

all	All categories.
category <LOG_CATEGORY_NAME>	Specify category. Log category name. Example: <i>Firewall</i>
group <LOG_GROUP_NAME>	Specify group. Group name. Example: <i>Firewall Event</i>
event <LOG_EVENT_NAME>	Specify event. Event name. Example: <i>Activate Firewall</i>
event-id <LOG_EVENT_ID>	Specify event ID. Event id. Example: <i>200</i>

Example

```
reset event-count all
reset event-count category VPN
```

Syntax

```
custom-template-description <WORD>
```

Mode

Log Categories

Description

Set custom template description.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
custom-template-description "Current event log company specific default settings"
```

Syntax

no custom-template-description

Mode

Log Categories

Description

Clear custom template description.

Example

no custom-template-description

Syntax

logging-level { alert | critical | debug | emergency | error | inform | notice | warning }

Mode

Log Categories

Description

Set global logging level.

Options

<i>alert</i>	Alert.
<i>critical</i>	Critical.
<i>debug</i>	Debug.
<i>emergency</i>	Emergency.
<i>error</i>	Error.
<i>inform</i>	Inform.
<i>notice</i>	Notice.
<i>warning</i>	Warning.

Example

logging-level critical

Syntax

alert-level { alert | critical | emergency | error | warning }

Mode

Log Categories

Description

Set alert level.

Options

<i>alert</i>	Alert.
<i>critical</i>	Critical.
<i>emergency</i>	Emergency.
<i>error</i>	Error.
<i>warning</i>	Warning.

Example

```
alert-level critical
```

Syntax

```
global-category-attribute
```

Mode

Log Categories

Description

Enter global category attributes configuration mode.

Example

```
global-category-attribute
```

Syntax

```
priority-level { alert | critical | debug | emergency | error | inform | mixed | notice | warning }
```

Mode

Log Categories Global Attributes

Description

Set priority level.

Options

<i>alert</i>	Alert.
<i>critical</i>	Critical.
<i>debug</i>	Debug.
<i>emergency</i>	Emergency.
<i>error</i>	Error.
<i>inform</i>	Inform.
<i>mixed</i>	Mixed.
<i>notice</i>	Notice.
<i>warning</i>	Warning.

Example

```
priority-level critical
```

Syntax

```
log-monitor [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable display in Log Monitor of categories and optionally set redundancy filter.

Options

type	Type.
enabled	Enable.
mixed	Mixed.
redundancy-interval <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: 123

Example

```
log-monitor redundancy-interval 60
```

Syntax

```
no log-monitor [ redundancy-interval ]
```

Mode

Log Categories Global Attributes

Description

Disable display in Log Monitor of categories.

Options

redundancy-interval	Clear the redundancy interval.

Example

```
no log-monitor
```

Syntax

```
email-alert [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Categories Global Attributes

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

type	Type.
enabled	Enable.
mixed	Mixed.

redundancy-interval	Set the redundancy interval in seconds.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

email-alert redundancy-interval 60

Syntax

no email-alert [redundancy-interval]

Mode

Log Categories Global Attributes

Description

Disable send events as Email Alerts.

Options

redundancy-interval Clear the redundancy interval.

Example

no email-alert

Syntax

syslog [{ [type] { enabled | mixed } } | redundancy-interval <UINT32>]

Mode

Log Categories Global Attributes

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

type	Type.
enabled	Enable.
mixed	Mixed.
redundancy-interval	Set the redundancy interval in seconds.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

syslog redundancy-interval 60

Syntax

no syslog [redundancy-interval]

Mode

Log Categories Global Attributes

Description

Disable report events via Syslog.

Options

redundancy-interval Clear the redundancy interval.

Example

no syslog

Syntax

event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }

Mode

Log Categories Global Attributes

Description

Set syslog server profile of categories.

Options

- mixed** Mixed profile.
- syslog-server-profile** Specify the syslog server profile.
- <SYSLOG_SERVER_PROFILE>** Syslog server profile.

Example

event-profile syslog-server-profile 0

Syntax

ipfix [{ [type] { enabled | mixed } } | redundancy-interval <UINT32>]

Mode

Log Categories Global Attributes

Description

Enable ipfix of categories and optionally set redundancy filter.

Options

- type** Type.
- enabled** Enable.
- mixed** Mixed.
- redundancy-interval** Set the redundancy interval in seconds.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

ipfix redundancy-interval 60

Syntax

no ipfix [redundancy-interval]

Mode

Description

Disable ipfix of categories.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no ipfix
```

Syntax

```
log-digest [ enabled | mixed ]
```

Mode

Log Categories Global Attributes

Description

Include events in Log Digest.

Options

enabled Enable.

mixed Mixed.

Example

```
log-digest
```

Syntax

```
no log-digest
```

Mode

Log Categories Global Attributes

Description

Exclude events in Log Digest.

Example

```
no log-digest
```

Syntax

```
color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }
```

Mode

Log Categories Global Attributes

Description

Set the color of the category to be displayed in the Log Monitor.

Options

black	Black.
blue	Blue.
green	Green.
hex	Hex representation.
<HEX_UINT32>	Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i>
leave-unchanged	Leave the original color unchanged.
orange	Orange.
purple	Purple.
red	Red.
rgb	Red, green, blue scale.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
yellow	Yellow.

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
log-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Categories Global Attributes

Description

Set Email address of all log events to send log to.

Options

address	Specify the log Email address.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
leave-unchanged	Leave the original log email address unchanged.

Example

```
log-email address categoriesadmin@utm.local
```

Syntax

```
no log-email
```

Mode

Log Categories Global Attributes

Description

Clear Email address of all log events to send log to.

Example

```
no log-email
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Categories Global Attributes

Description

Set Alert Email address of all log events to send log to.

Options

address	Specify the alert Email address.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
leave-unchanged	Leave the original alert email address unchanged.

Example

```
alert-email address categoriesadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Categories Global Attributes

Description

Clear Alert Email address of all log events to send alert to.

Example

```
no alert-email
```

Syntax

```
name <WORD>
```

Mode

Log Category
Log Group
Log Event

Description

log category/group/event name.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
name VPN
```

Syntax

id <UINT32>

Mode

Log Category
Log Group
Log Event

Description

log group/event ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

id 9

Syntax

priority-level { *alert* | *critical* | *debug* | *emergency* | *error* | *inform* | *mixed* | *notice* | *warning* }

Mode

Log Category

Description

Set priority level.

Options

<i>alert</i>	Alert.
<i>critical</i>	Critical.
<i>debug</i>	Debug.
<i>emergency</i>	Emergency.
<i>error</i>	Error.
<i>inform</i>	Inform.
<i>mixed</i>	Mixed.
<i>notice</i>	Notice.
<i>warning</i>	Warning.

Example

priority-level critical

Syntax

log-monitor [{ [*type*] { *enabled* | *mixed* } } | *redundancy-interval* <UINT32>]

Mode

Log Category

Description

Enable display in Log Monitor of category and optionally set redundancy filter.

Options

<i>type</i>	Type.
<i>enabled</i>	Enable.
<i>mixed</i>	Events under this are of mixed settings.
<i>redundancy-interval</i> <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

```
log-monitor redundancy-interval 60
log-monitor mixed
```

Syntax

```
no log-monitor [ redundancy-interval ]
```

Mode

Log Category

Description

Disable display in Log Monitor.

Options

<i>redundancy-interval</i>	Clear the redundancy interval.

Example

```
no log-monitor
```

Syntax

```
email-alert [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

<i>type</i>	Type.
<i>enabled</i>	Enable.
<i>mixed</i>	Events under this are of mixed settings.
<i>redundancy-interval</i> <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert [ redundancy-interval ]
```

Mode

Log Category

Description

Disable send events as Email Alerts.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no email-alert
```

Syntax

```
syslog [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

- type** Type.
- enabled** Enable.
- mixed** Events under this are of mixed settings.
- redundancy-interval** Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
syslog redundancy-interval 60
```

Syntax

```
no syslog [ redundancy-interval ]
```

Mode

Log Category

Description

Disable report events via Syslog.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no syslog
```

Syntax

```
event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }
```

Mode

Log Category

Description

Set syslog server profile of category.

Options

mixed	Mixed profile.
syslog-server-profile	Specify the syslog server profile.
<SYSLOG_SERVER_PROFILE>	Syslog server profile.

Example

```
event-profile syslog-server-profile 0
```

Syntax

```
log view option { application { { apply | block-cat | http-op | http-result | url } } | connection { { access-rule | idp-  
priority | idp-rule | nat-policy | rx-bytes | session-time | session-type | tx-bytes | user-name | vpn-policy } } | default |  
general { { category | event | group | id | message | msg-type | priority | time } } | interface { { destination | dst-int |  
dst-ip | dst-mac | dst-port | dst-vendor | dst-zone | ether-type | source | src-int | src-ip | src-mac | src-port | src-vendor  
| src-zone } } | other { { fw-action | notes } } | protocol { { dst-name | dst-nat-ip | dst-nat-port | icmp-code | icmp-type |  
in-protocol | in-spi | out-spi | src-name | src-nat-ip | src-nat-port } } }
```

Mode

Config

Description

Display view option settings.

Options

application	Enable view log application option settings.
apply	Apply.
block-cat	Block-cat.
http-op	Http-op.
http-result	Http-result.
url	Url.
connection	Enable view log connection option settings.
access-rule	Access-rule.
idp-priority	Idp-priority.
idp-rule	Idp-rule.

<i>nat-policy</i>	Nat-policy.
<i>rx-bytes</i>	Rx-bytes.
<i>session-time</i>	Session-time.
<i>session-type</i>	Session-type.
<i>tx-bytes</i>	Tx-bytes.
<i>user-name</i>	User-name.
<i>vpn-policy</i>	Vpn-policy.
<i>default</i>	Enable view log default option settings.
<i>general</i>	Enable view log general option settings.
<i>category</i>	Category.
<i>event</i>	Event.
<i>group</i>	Group.
<i>id</i>	ID.
<i>message</i>	Message.
<i>msg-type</i>	Msg-type.
<i>priority</i>	Priority.
<i>time</i>	Time.
<i>interface</i>	Enable view log interface option settings.
<i>destination</i>	Destination.
<i>dst-int</i>	Dst-int.
<i>dst-ip</i>	Dst-ip.
<i>dst-mac</i>	Dst-mac.
<i>dst-port</i>	Dst-port.
<i>dst-vendor</i>	Dst-vendor.
<i>dst-zone</i>	Dst-zone.
<i>ether-type</i>	Ether-type.
<i>source</i>	Source.
<i>src-int</i>	Src-int.
<i>src-ip</i>	Src-ip.
<i>src-mac</i>	Src-mac.
<i>src-port</i>	Src-port.
<i>src-vendor</i>	Src-vendor.
<i>src-zone</i>	Src-zone.
<i>other</i>	Enable view log other option settings.

<i>fw-action</i>	Fw-action.
<i>notes</i>	Notes.
<i>protocol</i>	Enable view log protocol option settings.
<i>dst-name</i>	Dst-name.
<i>dst-nat-ip</i>	Dst-nat-ip.
<i>dst-nat-port</i>	Dst-nat-port.
<i>icmp-code</i>	Icmp-code.
<i>icmp-type</i>	Icmp-type.
<i>in-protocol</i>	In-protocol.
<i>in-spi</i>	In-spi.
<i>out-spi</i>	Out-spi.
<i>src-name</i>	Src-name.
<i>src-nat-ip</i>	Src-nat-ip.
<i>src-nat-port</i>	Src-nat-port.

Example

```
log view option general time
```

Syntax

```
no log view option { { apply | block-cat | http-op | http-result | url } } | connection { { access-rule | idp-
priority | idp-rule | nat-policy | rx-bytes | session-time | session-type | tx-bytes | user-name | vpn-policy } } | general {
{ category | event | group | id | message | msg-type | priority | time } } | interface { { destination | dst-int | dst-ip |
dst-mac | dst-port | dst-vendor | dst-zone | ether-type | source | src-int | src-ip | src-mac | src-port | src-vendor | src-
zone } } | other { { fw-action | notes } } | protocol { { dst-name | dst-nat-ip | dst-nat-port | icmp-code | icmp-type | in-
protocol | in-spi | out-spi | src-name | src-nat-ip | src-nat-port } } }
```

Mode

Config

Description

Display view option settings.

Options

<i>application</i>	Enable view log application option settings.
<i>apply</i>	Apply.
<i>block-cat</i>	Block-cat.
<i>http-op</i>	Http-op.
<i>http-result</i>	Http-result.
<i>url</i>	Url.
<i>connection</i>	Enable view log connection option settings.
<i>access-rule</i>	Access-rule.

<i>idp-priority</i>	Idp-priority.
<i>idp-rule</i>	Idp-rule.
<i>nat-policy</i>	Nat-policy.
<i>rx-bytes</i>	Rx-bytes.
<i>session-time</i>	Session-time.
<i>session-type</i>	Session-type.
<i>tx-bytes</i>	Tx-bytes.
<i>user-name</i>	User-name.
<i>vpn-policy</i>	Vpn-policy.
<i>general</i>	Enable view log general option settings.
<i>category</i>	Category.
<i>event</i>	Event.
<i>group</i>	Group.
<i>id</i>	ID.
<i>message</i>	Message.
<i>msg-type</i>	Msg-type.
<i>priority</i>	Priority.
<i>time</i>	Time.
<i>interface</i>	Enable view log interface option settings.
<i>destination</i>	Destination.
<i>dst-int</i>	Dst-int.
<i>dst-ip</i>	Dst-ip.
<i>dst-mac</i>	Dst-mac.
<i>dst-port</i>	Dst-port.
<i>dst-vendor</i>	Dst-vendor.
<i>dst-zone</i>	Dst-zone.
<i>ether-type</i>	Ether-type.
<i>source</i>	Source.
<i>src-int</i>	Src-int.
<i>src-ip</i>	Src-ip.
<i>src-mac</i>	Src-mac.
<i>src-port</i>	Src-port.
<i>src-vendor</i>	Src-vendor.
<i>src-zone</i>	Src-zone.

<i>other</i>	Enable view log other option settings.
<i>fw-action</i>	Fw-action.
<i>notes</i>	Notes.
<i>protocol</i>	Enable view log protocol option settings.
<i>dst-name</i>	Dst-name.
<i>dst-nat-ip</i>	Dst-nat-ip.
<i>dst-nat-port</i>	Dst-nat-port.
<i>icmp-code</i>	Icmp-code.
<i>icmp-type</i>	Icmp-type.
<i>in-protocol</i>	In-protocol.
<i>in-spi</i>	In-spi.
<i>out-spi</i>	Out-spi.
<i>src-name</i>	Src-name.
<i>src-nat-ip</i>	Src-nat-ip.
<i>src-nat-port</i>	Src-nat-port.

Example

```
no log view option general time
```

Syntax

```
ipfix [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Category

Description

Enable ipfix of category and optionally set redundancy filter.

Options

<i>type</i>	Type.
<i>enabled</i>	Enable.
<i>mixed</i>	Categories under this are of mixed settings.
<i>redundancy-interval</i> <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123

Example

```
ipfix redundancy-interval 60
```

Syntax

```
no ipfix [ redundancy-interval ]
```

Mode

Log Category

Description

Disable ipfix of category.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no ipfix
```

Syntax

```
log-digest [ enabled | mixed ]
```

Mode

Log Category

Description

Include events in Log Digest.

Options

enabled Enable.

mixed Events under this are of mixed settings.

Example

```
log-digest
```

Syntax

```
no log-digest
```

Mode

Log Category

Description

Exclude events in Log Digest.

Example

```
no log-digest
```

Syntax

```
color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }
```

Mode

Log Category

Description

Set the color of the category to be displayed in the Log Monitor.

Options

<i>black</i>	Black.
<i>blue</i>	Blue.
<i>green</i>	Green.
<i>hex</i>	Hex representation.
<i><HEX_UINT32></i>	Hexadecimal integer in the form: 0xHHHHHHHHH. Example: <i>0xaa55aa55</i>
<i>leave-unchanged</i>	Leave unchanged.
<i>orange</i>	Orange.
<i>purple</i>	Purple.
<i>red</i>	Red.
<i>rgb</i>	Red, green, blue scale.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>yellow</i>	Yellow.

Example

```
color black
color leave-unchanged
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
log-email <EMAIL>
```

Mode

Log Category

Description

Set e-mail address to send log of this category to.

Options

<i><EMAIL></i>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>

Example

```
log-email categoryadmin@utm.local
```

Syntax

```
no log-email
```

Mode

Log Category

Description

Clear e-mail address to send log of this category to.

Example

```
no log-email
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Category

Description

Set alert e-mail address to send category to.

Options

address	Specify the alert e-mail address.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
leave-unchanged	Leave the original setting for children categories unchanged.

Example

```
alert-email address categoryadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Category

Description

Clear e-mail address to send alert of this category to.

Example

```
no alert-email
```

Syntax

```
category <WORD>
```

Mode

Log Group
Log Event

Description

log category name.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
category VPN
```

Syntax

priority-level { alert | critical | debug | emergency | error | inform | mixed | notice | warning }

Mode

Log Group

Description

Set priority level.

Options

<i>alert</i>	Alert.
<i>critical</i>	Critical.
<i>debug</i>	Debug.
<i>emergency</i>	Emergency.
<i>error</i>	Error.
<i>inform</i>	Inform.
<i>mixed</i>	Mixed.
<i>notice</i>	Notice.
<i>warning</i>	Warning.

Example

priority-level critical

Syntax

log-monitor [{ [type] { enabled | mixed } } | redundancy-interval <UINT32>]

Mode

Log Group

Description

Enable display in Log Monitor of group and optionally set redundancy filter.

Options

<i>type</i>	Type.
<i>enabled</i>	Enable.
<i>mixed</i>	Events under this are of mixed settings.
<i>redundancy-interval</i> <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

log-monitor redundancy-interval 60
log-monitor mixed

Syntax

```
no log-monitor [ redundancy-interval ]
```

Mode

Log Group

Description

Disable display in Log Monitor.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no log-monitor
```

Syntax

```
email-alert [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

<i>type</i>	Type.
<i>enabled</i>	Enable.
<i>mixed</i>	Events under this are of mixed settings.
<i>redundancy-interval</i> <i><UINT32></i>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert [ redundancy-interval ]
```

Mode

Log Group

Description

Disable send events as Email Alerts.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no email-alert
```

Syntax

```
syslog [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

type	Type.
enabled	Enable.
mixed	Events under this are of mixed settings.
redundancy-interval <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: 123

Example

```
syslog redundancy-interval 60
```

Syntax

```
no syslog [ redundancy-interval ]
```

Mode

Log Group

Description

Disable report events via Syslog.

Options

redundancy-interval	Clear the redundancy interval.

Example

```
no syslog
```

Syntax

```
event-profile { mixed | syslog-server-profile <SYSLOG_SERVER_PROFILE> }
```

Mode

Log Group

Description

Set syslog server profile of group.

Options

mixed	Mixed profile.
syslog-server-profile <SYSLOG_SERVER_PROFILE>	Specify the syslog server profile. Syslog server profile.

Example

Syntax

```
ipfix [ { [ type ] { enabled | mixed } } | redundancy-interval <UINT32> ]
```

Mode

Log Group

Description

Enable ipfix of group and optionally set redundancy filter.

Options

type	Type.
enabled	Enable.
mixed	Categories under this are of mixed settings.
redundancy-interval <UINT32>	Set the redundancy interval in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
ipfix redundancy-interval 60
```

Syntax

```
no ipfix [ redundancy-interval ]
```

Mode

Log Group

Description

Disable ipfix of group.

Options

redundancy-interval Clear the redundancy interval.

Example

```
no ipfix
```

Syntax

```
log-digest [ enabled | mixed ]
```

Mode

Log Group

Description

Include events in Log Digest.

Options

enabled Enable.

mixed Events under this are of mixed settings.

Example

log-digest

Syntax

no log-digest

Mode

Log Group

Description

Exclude events in Log Digest.

Example

no log-digest

Syntax

color { black | blue | green | hex <HEX_UINT32> | leave-unchanged | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }

Mode

Log Group

Description

Set the color of the group to be displayed in the Log Monitor.

Options

<i>black</i>	Black.
<i>blue</i>	Blue.
<i>green</i>	Green.
<i>hex</i> <i><HEX_UINT32></i>	Hex representation. Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i>
<i>leave-unchanged</i>	Leave unchanged.
<i>orange</i>	Orange.
<i>purple</i>	Purple.
<i>red</i>	Red.
<i>rgb</i> <i><UINT8></i>	Red, green, blue scale. Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>yellow</i>	Yellow.

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
alert-email { address <EMAIL> | leave-unchanged }
```

Mode

Log Group

Description

Set alert e-mail address to send group to.

Options

address	Specify the alert e-mail address.
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
leave-unchanged	Leave the original setting for children categories unchanged.

Example

```
alert-email address groupadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Group

Description

Clear e-mail address to send alert of this group to.

Example

```
no alert-email
```

Syntax

```
group <WORD>
```

Mode

Log Event

Description

log group name.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
group API
```

Syntax

priority-level { alert | critical | debug | emergency | error | inform | notice | warning }

Mode

Log Event

Description

Set priority level.

Options

- alert** Alert.
- critical** Critical.
- debug** Debug.
- emergency** Emergency.
- error** Error.
- inform** Inform.
- notice** Notice.
- warning** Warning.

Example

priority-level critical

Syntax

log-monitor [redundancy-interval <UINT32>]

Mode

Log Event

Description

Enable display in Log Monitor of event and optionally set redundancy filter.

Options

- redundancy-interval** Set the redundancy interval in seconds.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

log-monitor redundancy-interval 60
log-monitor

Syntax

no log-monitor

Mode

Log Event

Description

Disable display in Log Monitor.

Example

```
no log-monitor
```

Syntax

```
email-alert [ redundancy-interval <UINT32> ]
```

Mode

Log Event

Description

Enable send events as Email Alerts and optionally set redundancy filter.

Options

<i>redundancy-interval</i>	Set the redundancy interval in seconds.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
email-alert redundancy-interval 60
```

Syntax

```
no email-alert
```

Mode

Log Event

Description

Disable send events as Email Alerts.

Example

```
no email-alert
```

Syntax

```
syslog [ redundancy-interval <UINT32> ]
```

Mode

Log Event

Description

Enable report events via Syslog and optionally set redundancy filter.

Options

<i>redundancy-interval</i>	Set the redundancy interval in seconds.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

Example

```
syslog redundancy-interval 60
```

Syntax


```
no syslog
```

Mode

Log Event

Description

Disable report events via Syslog.

Example

```
no syslog
```

Syntax

```
event-profile syslog-server-profile <SYSLOG_SERVER_PROFILE>
```

Mode

Log Event

Description

Set syslog server profile of event.

Options

<SYSLOG_SERVER_PROFILE> Syslog server profile.

Example

```
event-profile syslog-server-profile 0
```

Syntax

```
ipfix [ redundancy-interval <UINT32> ]
```

Mode

Log Event

Description

Enable ipfix of event and optionally set redundancy filter.

Options

redundancy-interval Set the redundancy interval in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
ipfix redundancy-interval 60
```

Syntax

```
no ipfix
```

Mode

Log Event

Description

Disable ipfix of event.

Example

no ipfix

Syntax

log-digest

Mode

Log Event

Description

Include events in Log Digest.

Example

log-digest

Syntax

no log-digest

Mode

Log Event

Description

Exclude events in Log Digest.

Example

no log-digest

Syntax

color { black | blue | green | hex <HEX_UINT32> | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }

Mode

Log Event

Description

Set the color of the event to be displayed in the Log Monitor.

Options

black	Black.
blue	Blue.
green	Green.
hex <HEX_UINT32>	Hex representation. Hexadecimal integer in the form: 0xHHHHHHHH. Example: 0xaa55aa55
orange	Orange.
purple	Purple.
red	Red.
rgb <UINT8>	Red, green, blue scale. Integer in the form: D OR 0xHH.

	Example: <i>123</i>
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
yellow	Yellow.

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
alert-email address <EMAIL>
```

Mode

Log Event

Description

Set alert e-mail address to send event to.

Options

- address** Specify the alert e-mail address.
- <EMAIL>** E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
alert-email address eventadmin@utm.local
```

Syntax

```
no alert-email
```

Mode

Log Event

Description

Clear e-mail address to send alert of this event to.

Example

```
no alert-email
```

Syntax

```
facility { authpriv-messages | clock-daemon-linux-bsd | clock-daemon-solaris | ftp-daemon | generated-internally | kernel |
line-printer-subsystem | local-use0 | local-use1 | local-use2 | local-use3 | local-use4 | local-use5 | local-use6 | local-use7
| log-alert | log-audit | mail-system | network-news-subsystem | ntp-subsystem | security-authorization-messages | system-
daemons | user-level-messages | uucp-subsystem }
```

Mode

Syslog

Description

Set syslog facility for all the servers.

Options

<i>authpriv-messages</i>	AUTHPRIV security/authorization messages.
<i>clock-daemon-linux-bsd</i>	Clock daemon (BSP,Linux).
<i>clock-daemon-solaris</i>	Clock daemon (solaris).
<i>ftp-daemon</i>	FTP daemon.
<i>generated-internally</i>	Messages generated internally by syslogd.
<i>kernel</i>	Kernel.
<i>line-printer-subsystem</i>	Line printer subsystem.
<i>local-use0</i>	Local use 0.
<i>local-use1</i>	Local use 1.
<i>local-use2</i>	Local use 2.
<i>local-use3</i>	Local use 3.
<i>local-use4</i>	Local use 4.
<i>local-use5</i>	Local use 5.
<i>local-use6</i>	Local use 6.
<i>local-use7</i>	Local use 7.
<i>log-alert</i>	Log alert.
<i>log-audit</i>	Log audit.
<i>mail-system</i>	Mail system.
<i>network-news-subsystem</i>	Network news subsystem.
<i>ntp-subsystem</i>	NTP subsystem.
<i>security-authorization-messages</i>	Security/authorization messages.
<i>system-daemons</i>	System daemons.
<i>user-level-messages</i>	User-level messages.
<i>uucp-subsystem</i>	UUCP subsystem.

Example

facility local-use0

Syntax

format { arcSight | default | enhanced-syslog | webtrends }

Mode

Syslog

Description

Set syslog format for all the servers.

Options

<i>arcSight</i>	Arcsight format.
<i>default</i>	Default format.
<i>enhanced-syslog</i>	Enhanced syslog format.
<i>webtrends</i>	Webtrends format.

Example

format default

Syntax

id <WORD>

Mode

Syslog

Description

Set syslog ID for all the servers.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

id firewall

Syntax

event-rate-limiting <UINT16>

Mode

Syslog

Description

Set maximum events per second for all the servers.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

event-rate-limiting 1000

Syntax

no event-rate-limiting

Mode

Syslog

Description

Clear maximum events per second for all the servers.

Example

no event-rate-limiting

Syntax

data-rate-limiting <UINT32>

Mode

Syslog

Description

Set maximum bytes per second for all the servers.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

data-rate-limiting 100000000

Syntax

no data-rate-limiting

Mode

Syslog

Description

Clear maximum bytes per second for all the servers.

Example

no data-rate-limiting

Syntax

enhanced general { category | event-id | group-category | host | message }

Mode

Syslog

Description

Enable enhanced syslog general settings.

Options

category Category.

event-id Event ID.

group-category Group category.

host Host.

message Message.

Example

enhanced general host

Syntax

```
no enhanced general { category | event-id | group-category | host | message }
```

Mode

Syslog

Description

Disable enhanced syslog general fields settings.

Options

<i>category</i>	Category.
<i>event-id</i>	Event ID.
<i>group-category</i>	Group category.
<i>host</i>	Host.
<i>message</i>	Message.

Example

```
no enhanced general host
```

Syntax

```
enhanced interface { destination | dst-mac | source | src-mac }
```

Mode

Syslog

Description

Enable enhanced syslog interface fields settings.

Options

<i>destination</i>	Destination interface.
<i>dst-mac</i>	Destination MAC address.
<i>source</i>	Source interface.
<i>src-mac</i>	Source MAC address.

Example

```
enhanced interface source
```

Syntax

```
no enhanced interface { destination | dst-mac | source | src-mac }
```

Mode

Syslog

Description

Disable enhanced syslog interface fields settings.

Options

<i>destination</i>	Destination interface.
<i>dst-mac</i>	Destination MAC address.
<i>source</i>	Source interface.
<i>src-mac</i>	Source MAC address.

Example

```
no enhanced interface source
```

Syntax

```
enhanced protocol { dst-ip | dst-nat | dst-nat-port | dst-port | icmp-code | icmp-type | protocol | src-ip | src-nat | src-nat-port | src-port }
```

Mode

Syslog

Description

Enable enhanced syslog protocol fields settings.

Options

<i>dst-ip</i>	Destination IP.
<i>dst-nat</i>	Destination NAT IP.
<i>dst-nat-port</i>	Destination NAT port.
<i>dst-port</i>	Destination port.
<i>icmp-code</i>	ICMP code.
<i>icmp-type</i>	ICMP type.
<i>protocol</i>	Protocol.
<i>src-ip</i>	Source IP.
<i>src-nat</i>	Source NAT IP.
<i>src-nat-port</i>	Source NAT port.
<i>src-port</i>	Source port.

Example

```
enhanced protocol src-ip
```

Syntax

```
no enhanced protocol { dst-ip | dst-nat | dst-nat-port | dst-port | icmp-code | icmp-type | protocol | src-ip | src-nat | src-nat-port | src-port }
```

Mode

Syslog

Description

Disable enhanced syslog protocol fields settings.

Options

<i>dst-ip</i>	Destination IP.
<i>dst-nat</i>	Destination NAT IP.
<i>dst-nat-port</i>	Destination NAT port.
<i>dst-port</i>	Destination port.
<i>icmp-code</i>	ICMP code.
<i>icmp-type</i>	ICMP type.
<i>protocol</i>	Protocol.
<i>src-ip</i>	Source IP.
<i>src-nat</i>	Source NAT IP.
<i>src-nat-port</i>	Source NAT port.
<i>src-port</i>	Source port.

Example

```
no enhanced protocol src-ip
```

Syntax

```
enhanced connection { bytes-rcvd | bytes-sent | client-policy | conn-duration | dst-vpn | dst-zone | interface-stats | pkts-rcvd | pkts-sent | session-time | session-type | sonicpoint-stats | src-vpn | src-zone | user }
```

Mode

Syslog

Description

Enable enhanced syslog connection fields settings.

Options

<i>bytes-rcvd</i>	Bytes received.
<i>bytes-sent</i>	Bytes send.
<i>client-policy</i>	Client policy.
<i>conn-duration</i>	Connection duration.
<i>dst-vpn</i>	Destination VPN policy.
<i>dst-zone</i>	Destination zone.
<i>interface-stats</i>	Interface statistics.
<i>pkts-rcvd</i>	Packets received.
<i>pkts-sent</i>	Packets send.
<i>session-time</i>	Session time.

<i>session-type</i>	Session type.
<i>sonicpoint-stats</i>	Sonicpoint statistics.
<i>src-vpn</i>	Source VPN policy.
<i>src-zone</i>	Source zone.
<i>user</i>	User.

Example

```
enhanced connection user
```

Syntax

```
no enhanced connection { bytes-rcvd | bytes-sent | client-policy | conn-duration | dst-vpn | dst-zone | interface-stats |
pkts-rcvd | pkts-sent | session-time | session-type | sonicpoint-stats | src-vpn | src-zone | user }
```

Mode

Syslog

Description

Disable enhanced syslog connection fields settings.

Options

<i>bytes-rcvd</i>	Bytes received.
<i>bytes-sent</i>	Bytes send.
<i>client-policy</i>	Client policy.
<i>conn-duration</i>	Connection duration.
<i>dst-vpn</i>	Destination VPN policy.
<i>dst-zone</i>	Destination zone.
<i>interface-stats</i>	Interface statistics.
<i>pkts-rcvd</i>	Packets received.
<i>pkts-sent</i>	Packets send.
<i>session-time</i>	Session time.
<i>session-type</i>	Session type.
<i>sonicpoint-stats</i>	Sonicpoint statistics.
<i>src-vpn</i>	Source VPN policy.
<i>src-zone</i>	Source zone.
<i>user</i>	User.

Example

```
no enhanced connection user
```

Syntax

```
enhanced application { app | block-reason | gms-heartbeat | gms-url | http-operation | http-result | url }
```

Mode

Syslog

Description

Enable enhanced syslog application fields settings.

Options

app	Application.
block-reason	Block reason.
gms-heartbeat	GMS heart beat.
gms-url	GMS change URL.
http-operation	HTTP operation.
http-result	HTTP result.
url	URL.

Example

```
enhanced application url
```

Syntax

```
no enhanced application { app | block-reason | gms-heartbeat | gms-url | http-operation | http-result | url }
```

Mode

Syslog

Description

Disable enhanced syslog application fields settings.

Options

app	Application.
block-reason	Block reason.
gms-heartbeat	GMS heart beat.
gms-url	GMS change URL.
http-operation	HTTP operation.
http-result	HTTP result.
url	URL.

Example

```
no enhanced application url
```

Syntax

```
enhanced others { anti-spam | app-firewall | counter | file-id | file-tx | idp | note | npcs | raw-data | rule-action | uuid }
```

Mode

Syslog

Description

Enable enhanced syslog others fields settings.

Options

<i>anti-spam</i>	Anti-spam.
<i>app-firewall</i>	App firewall.
<i>counter</i>	Counter.
<i>file-id</i>	File ID.
<i>file-tx</i>	File TX status.
<i>idp</i>	IDP.
<i>note</i>	Note.
<i>npcs</i>	NPCS.
<i>raw-data</i>	Raw data.
<i>rule-action</i>	Rule action.
<i>uuid</i>	UUID.

Example

```
enhanced others idp
```

Syntax

```
no enhanced others { anti-spam | app-firewall | counter | file-id | file-tx | idp | note | npcs | raw-data | rule-action |  
uuid }
```

Mode

Syslog

Description

Disable enhanced syslog others fields settings.

Options

<i>anti-spam</i>	Anti-spam.
<i>app-firewall</i>	App firewall.
<i>counter</i>	Counter.
<i>file-id</i>	File ID.
<i>file-tx</i>	File TX status.
<i>idp</i>	IDP.
<i>note</i>	Note.

<i>npcs</i>	NPCS.
<i>raw-data</i>	Raw data.
<i>rule-action</i>	Rule action.
<i>uuid</i>	UUID.

Example

no enhanced others idp

Syntax

arcsight general { category | event-id | group-category | host | message }

Mode

Syslog

Description

Enable arcsight syslog general settings.

Options

<i>category</i>	Category.
<i>event-id</i>	Event ID.
<i>group-category</i>	Group category.
<i>host</i>	Host.
<i>message</i>	Message.

Example

arcsight general host

Syntax

no arcsight general { category | event-id | group-category | host | message }

Mode

Syslog

Description

Disable arcsight syslog general fields settings.

Options

<i>category</i>	Category.
<i>event-id</i>	Event ID.
<i>group-category</i>	Group category.
<i>host</i>	Host.
<i>message</i>	Message.

Example

```
no arcsight general host
```

Syntax

```
arcsight interface { destination | dst-mac | source | src-mac }
```

Mode

Syslog

Description

Enable arcsight syslog interface fields settings.

Options

destination Destination interface.

dst-mac Destination MAC address.

source Source interface.

src-mac Source MAC address.

Example

```
arcsight interface source
```

Syntax

```
no arcsight interface { destination | dst-mac | source | src-mac }
```

Mode

Syslog

Description

Disable arcsight syslog interface fields settings.

Options

destination Destination interface.

dst-mac Destination MAC address.

source Source interface.

src-mac Source MAC address.

Example

```
no arcsight interface source
```

Syntax

```
arcsight protocol { dst-ip | dst-nat | dst-nat-port | dst-port | icmp-code | icmp-type | protocol | src-ip | src-nat | src-nat-port | src-port }
```

Mode

Syslog

Description

Enable arcsight syslog protocol fields settings.

Options

<i>dst-ip</i>	Destination IP.
<i>dst-nat</i>	Destination NAT IP.
<i>dst-nat-port</i>	Destination NAT port.
<i>dst-port</i>	Destination port.
<i>icmp-code</i>	ICMP code.
<i>icmp-type</i>	ICMP type.
<i>protocol</i>	Protocol.
<i>src-ip</i>	Source IP.
<i>src-nat</i>	Source NAT IP.
<i>src-nat-port</i>	Source NAT port.
<i>src-port</i>	Source port.

Example

```
arcsight protocol src-ip
```

Syntax

```
no arcsight protocol { dst-ip | dst-nat | dst-nat-port | dst-port | icmp-code | icmp-type | protocol | src-ip | src-nat | src-nat-port | src-port }
```

Mode

Syslog

Description

Disable arcsight syslog protocol fields settings.

Options

<i>dst-ip</i>	Destination IP.
<i>dst-nat</i>	Destination NAT IP.
<i>dst-nat-port</i>	Destination NAT port.
<i>dst-port</i>	Destination port.
<i>icmp-code</i>	ICMP code.
<i>icmp-type</i>	ICMP type.
<i>protocol</i>	Protocol.
<i>src-ip</i>	Source IP.
<i>src-nat</i>	Source NAT IP.
<i>src-nat-port</i>	Source NAT port.
<i>src-port</i>	Source port.

Example

```
no arcsight protocol src-ip
```

Syntax

```
arcsight connection { bytes-rcvd | bytes-sent | client-policy | conn-duration | dst-vpn | dst-zone | interface-stats | pkts-rcvd | pkts-sent | session-time | session-type | sonicpoint-stats | src-vpn | src-zone | user }
```

Mode

Syslog

Description

Enable arcsight syslog connection fields settings.

Options

<i>bytes-rcvd</i>	Bytes received.
<i>bytes-sent</i>	Bytes send.
<i>client-policy</i>	Client policy.
<i>conn-duration</i>	Connection duration.
<i>dst-vpn</i>	Destination VPN policy.
<i>dst-zone</i>	Destination zone.
<i>interface-stats</i>	Interface statistics.
<i>pkts-rcvd</i>	Packets received.
<i>pkts-sent</i>	Packets send.
<i>session-time</i>	Session time.
<i>session-type</i>	Session type.
<i>sonicpoint-stats</i>	Sonicpoint statistics.
<i>src-vpn</i>	Source VPN policy.
<i>src-zone</i>	Source zone.
<i>user</i>	User.

Example

```
arcsight connection user
```

Syntax

```
no arcsight connection { bytes-rcvd | bytes-sent | client-policy | conn-duration | dst-vpn | dst-zone | interface-stats | pkts-rcvd | pkts-sent | session-time | session-type | sonicpoint-stats | src-vpn | src-zone | user }
```

Mode

Syslog

Description

Disable arcsight syslog connection fields settings.

Options

<i>bytes-rcvd</i>	Bytes received.
<i>bytes-sent</i>	Bytes send.
<i>client-policy</i>	Client policy.
<i>conn-duration</i>	Connection duration.
<i>dst-vpn</i>	Destination VPN policy.
<i>dst-zone</i>	Destination zone.
<i>interface-stats</i>	Interface statistics.
<i>pkts-rcvd</i>	Packets received.
<i>pkts-sent</i>	Packets send.
<i>session-time</i>	Session time.
<i>session-type</i>	Session type.
<i>sonicpoint-stats</i>	Sonicpoint statistics.
<i>src-vpn</i>	Source VPN policy.
<i>src-zone</i>	Source zone.
<i>user</i>	User.

Example

```
no arcsight connection user
```

Syntax

```
arcsight application { app | block-reason | gms-heartbeat | gms-url | http-operation | http-result | url }
```

Mode

Syslog

Description

Enable arcsight syslog application fields settings.

Options

<i>app</i>	Application.
<i>block-reason</i>	Block reason.
<i>gms-heartbeat</i>	GMS heart beat.
<i>gms-url</i>	GMS change URL.
<i>http-operation</i>	HTTP operation.
<i>http-result</i>	HTTP result.
<i>url</i>	URL.

Example

```
arcsight application url
```

Syntax

```
no arcsight application { app | block-reason | gms-heartbeat | gms-url | http-operation | http-result | url }
```

Mode

Syslog

Description

Disable arcsight syslog application fields settings.

Options

app	Application.
block-reason	Block reason.
gms-heartbeat	GMS heart beat.
gms-url	GMS change URL.
http-operation	HTTP operation.
http-result	HTTP result.
url	URL.

Example

```
no arcsight application url
```

Syntax

```
arcsight others { anti-spam | app-firewall | counter | file-id | file-tx | idp | note | npcs | raw-data | rule-action | uuid }
```

Mode

Syslog

Description

Enable arcsight syslog others fields settings.

Options

anti-spam	Anti-spam.
app-firewall	App firewall.
counter	Counter.
file-id	File ID.
file-tx	File TX status.
idp	IDP.
note	Note.
npcs	NPCS.
raw-data	Raw data.

rule-action Rule action.

uuid UUID.

Example

```
arcsight others idp
```

Syntax

```
no arcsight others { anti-spam | app-firewall | counter | file-id | file-tx | idp | note | npcs | raw-data | rule-action |  
uuid }
```

Mode

Syslog

Description

Disable arcsight syslog others fields settings.

Options

anti-spam Anti-spam.

app-firewall App firewall.

counter Counter.

file-id File ID.

file-tx File TX status.

idp IDP.

note Note.

npcs NPCS.

raw-data Raw data.

rule-action Rule action.

uuid UUID.

Example

```
no arcsight others idp
```

Syntax

```
ndpp
```

Mode

Syslog

Description

Enable NDPP enforcement for syslog server.

Example

```
ndpp
```

Syntax

no ndpp

Mode

Syslog

Description

Disable NDPP enforcement for syslog server.

Example

no ndpp

Syntax

type { analyzer | syslog-server }

Mode

Syslog Server

Description

Syslog server type.

Options

analyzer Analyzer server

syslog-server Syslog server

Example

type analyzer

Syntax

facility { authpriv-messages | clock-daemon-linux-bsd | clock-daemon-solaris | ftp-daemon | generated-internally | kernel | line-printer-subsystem | local-use0 | local-use1 | local-use2 | local-use3 | local-use4 | local-use5 | local-use6 | local-use7 | log-alert | log-audit | mail-system | network-news-subsystem | ntp-subsystem | security-authorization-messages | system-daemons | user-level-messages | uucp-subsystem }

Mode

Syslog Server

Description

Syslog server facility.

Options

authpriv-messages	AUTHPRIV security/authorization messages.
clock-daemon-linux-bsd	Clock daemon (BSP,Linux).
clock-daemon-solaris	Clock daemon (solaris).
ftp-daemon	FTP daemon.
generated-internally	Messages generated internally by syslogd.
kernel	Kernel.
line-printer-subsystem	Line printer subsystem.

<i>local-use0</i>	Local use 0.
<i>local-use1</i>	Local use 1.
<i>local-use2</i>	Local use 2.
<i>local-use3</i>	Local use 3.
<i>local-use4</i>	Local use 4.
<i>local-use5</i>	Local use 5.
<i>local-use6</i>	Local use 6.
<i>local-use7</i>	Local use 7.
<i>log-alert</i>	Log alert.
<i>log-audit</i>	Log audit.
<i>mail-system</i>	Mail system.
<i>network-news-subsystem</i>	Network news subsystem.
<i>ntp-subsystem</i>	NTP subsystem.
<i>security-authorization-messages</i>	Security/authorization messages.
<i>system-daemons</i>	System daemons.
<i>user-level-messages</i>	User-level messages.
<i>uucp-subsystem</i>	UUCP subsystem.

Example

facility local-use0

Syntax

format { arcSight | default | enhanced-syslog | webtrends }

Mode

Syslog Server

Description

Syslog server format.

Options

<i>arcSight</i>	Arcsight format.
<i>default</i>	Default format.
<i>enhanced-syslog</i>	Enhanced syslog format.
<i>webtrends</i>	Webtrends format.

Example

format default

Syntax

id <WORD>

Mode

Syslog Server

Description

Syslog server ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

id firewall

Syntax

event-rate-limiting [*enabled* | *maximum-events* <UINT16>]

Mode

Syslog Server

Description

Enable syslog event rate limiting or set maximum events per second.

Options

enabled Enable syslog event rate limiting.

maximum-events Set maximum events per second.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

event-rate-limiting maximum-events 1000

Syntax

no event-rate-limiting [*maximum-events*]

Mode

Syslog Server

Description

Disable syslog event rate limiting or clear maximum events per second.

Options

maximum-events Clear maximum events per second.

Example

no event-rate-limiting

Syntax

```
data-rate-limiting [ enabled | maximum-bytes <UINT32> ]
```

Mode

Syslog Server

Description

Enable syslog data rate limiting or set maximum bytes per second.

Options

- enabled** Enable syslog data rate limiting.
- maximum-bytes <UINT32>** Set maximum bytes per second.
Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
data-rate-limiting maximum-bytes 100000000
```

Syntax

```
no data-rate-limiting [ maximum-bytes ]
```

Mode

Syslog Server

Description

Disable syslog data rate limiting or clear maximum bytes per second.

Options

- maximum-bytes** Clear maximum bytes per second.

Example

```
no data-rate-limiting
```

Syntax

```
enabled
```

Mode

Syslog Server

Description

Enable syslog server.

Example

```
enabled
```

Syntax

```
no enabled
```

Mode

Syslog Server

Description

Disable syslog server.

Example

```
no enabled
```

Syntax

```
no syslog-servers
```

Mode

Syslog

Description

Delete all syslog servers.

Example

```
no syslog-servers
```

Syntax

```
enable servers
```

Mode

Syslog

Description

Enable all syslog servers.

Example

```
enable servers
```

Syntax

```
no enable servers
```

Mode

Syslog

Description

Disable all syslog servers.

Example

```
no enable servers
```

Syntax

```
server address { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> } port <UINT32> profile  
<SYSLOG_SERVER_PROFILE>
```

Mode

Syslog
Analyzer
Viewpoint

Description

Add/edit syslog server.

Options

<i>fqdn</i>	Address object full qualified domain name (FQDN).
<i><ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	Address object host
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name
<i><ADDR_FQDNHOST_ADDR></i>	FQDN/host address object name. Example: <i>Web Server</i>
<i>port</i>	server port.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>profile</i>	Syslog server profile.
<i><SYSLOG_SERVER_PROFILE></i>	Syslog server profile.

Example

server address name "Syslog Server Public" port 514 profile 0
server address host 10.10.10.10 port 514 profile 0

Syntax

no server address name <SYSLOG_SERVER> port <SYSLOG_SERVER_PORT> profile <SYSLOG_SERVER_PROFILE>

Mode

Syslog
Analyzer
Viewpoint

Description

Delete syslog server.

Options

<i>name</i>	Address object name
<i><SYSLOG_SERVER></i>	Syslog custom server in the form: hostname OR a.b.c.d. Example: <i>abc</i>
<i>port</i>	server port.
<i><SYSLOG_SERVER_PORT></i>	Syslog custom server port. Example: <i>80</i>
<i>profile</i>	Syslog server profile.
<i><SYSLOG_SERVER_PROFILE></i>	Syslog server profile.

Example

no server address name "Syslog Server Public" port 514 profile 0

Syntax

no servers

Mode

Syslog
Analyzer
Viewpoint

Description

Delete all syslog servers.

Example

no servers

Syntax

profile <SYSLOG_SERVER_PROFILE>

Mode

Syslog Server

Description

Configure the syslog server profile.

Options

<SYSLOG_SERVER_PROFILE> Syslog server profile.

Example

profile 0

Syntax

no profile

Mode

Syslog Server

Description

Clear the syslog server profile.

Example

no profile

Syntax

address { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }

Mode

Syslog Server

Description

configure the syslog server name.

Options

fqdn <ADDR_FQDN>	Address object full qualified domain name (FQDN). FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
host <ADDR_HOST>	Address object host IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_FQDNHOST_ADDR>	Address object name FQDN/host address object name. Example: <i>Web Server</i>

Example

```
address name "Syslog Server Public"
address host 10.10.10.10
address fqdn "*.example.com"
```

Syntax

```
port <UINT32>
```

Mode

Syslog Server

Description

Configure the syslog server port.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
port 514
```

Syntax

```
no port
```

Mode

Syslog Server

Description

Clear the syslog server port.

Example

```
no port
```

Syntax

```
outbound-interface <SYSLOG_SERVER_OUTBOUND_INTERFACE>
```

Mode

Syslog Server

Description

Set the outbound interface.

Options

<SYSLOG_SERVER_OUTBOUND_INTERFACE> Syslog server outbound interface name.
Example: *vpnTunnelInterface*

Example

```
outbound-interface "Remote Office"
```

Syntax

```
no outbound-interface
```

Mode

Syslog Server

Description

Clear the outbound interface.

Example

```
no outbound-interface
```

Syntax

```
local-interface <NETMON_INTERFACE>
```

Mode

Syslog Server

Description

Set the local interface.

Options

<NETMON_INTERFACE> Interface name.
Example: *X0*

Example

```
local-interface X2
```

Syntax

```
no local-interface
```

Mode

Syslog Server

Description

Clear the local interface.

Example

```
no local-interface
```

Syntax

```
email-address { alert <EMAIL> | audit <EMAIL> | log <EMAIL> | user <EMAIL> }
```

Mode

Log Automation

Description

Set E-mail address.

Options

alert Set E-mail address to send alert to.
<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

audit Set E-mail address to send auditing records to.

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

log Set E-mail address to send log to.

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

user Set E-mail address to send user creation and enablement notification to.

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
email-address log admin@somedomain.com
email-address alert admin@somedomain.com
```

Syntax

```
no email-address { alert | audit | log | user }
```

Mode

Log Automation

Description

Clear E-mail address.

Options

alert Clear E-mail address to send alert to.

audit Clear E-mail address to send auditing records to.

log Clear E-mail address to send log to.

user Clear E-mail address to send user creation and enablement notification to.

Example

```
no email-address log
no email-address alert
```

Syntax

```
send-log { { daily hour <UINT8> minute <UINT8> | weekly { fri | mon | sat | sun | thu | tue | wed } hour <UINT8> minute <UINT8> | when-full } }
```

Mode

Log Automation

Description

Specify when to send log.

Options

daily Daily.

hour Hour.

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

minute Minute.

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

<i>weekly</i>	Weekly.
<i>fri</i>	Friday.
<i>mon</i>	Monday.
<i>sat</i>	Saturday.
<i>sun</i>	Sunday.
<i>thu</i>	Thursday.
<i>tue</i>	Tuesday.
<i>wed</i>	Wednesday.
<i>hour</i>	Hour.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>minute</i>	Minute.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>when-full</i>	When full.

Example

```
send-log weekly mon hour 07 minute 30
```

Syntax

```
email-format-log { csv | html | plain-text }
```

Mode

Log Automation

Description

Specify e-mail format for sending log.

Options

<i>csv</i>	CSV.
<i>html</i>	HTML.
<i>plain-text</i>	Plain text.

Example

```
email-format-log plain-text
```

Syntax

```
send-audit { { daily hour <UINT8> minute <UINT8> | weekly { fri | mon | sat | sun | thu | tue | wed } hour <UINT8> minute <UINT8> | when-full } }
```

Mode

Log Automation

Description

Specify when to send auditing records.

Options

daily	Daily.
hour	Hour.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
minute	Minute.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
weekly	Weekly.
fri	Friday.
mon	Monday.
sat	Saturday.
sun	Sunday.
thu	Thursday.
tue	Tuesday.
wed	Wednesday.
hour	Hour.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
minute	Minute.
<UINT8>	Integer in the form: D OR 0xHH. Example: <i>123</i>
when-full	When full.

Example

send-audit weekly mon hour 07 minute 30

Syntax

email-format-audit { csv | html | plain-text }

Mode

Log Automation

Description

Specify e-mail format for sending auditing records.

Options

csv	CSV.
html	HTML.
plain-text	Plain text.

Example

email-format-audit plain-text

Syntax

include-all-log-information

Mode

Description

Include all log information.

Example

```
include-all-log-information
```

Syntax

```
no include-all-log-information
```

Mode

Description

Include default log information.

Example

```
no include-all-log-information
```

Syntax

```
health-check-email { address <EMAIL> | body <WORD> | schedule { days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } | subject <WORD> }
```

Mode

Description

Edit health check E-mail settings.

Options

address <EMAIL>	Set the health check E-mail address. E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
body <WORD>	Set the health check E-mail body. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
schedule	Enable E-mail health check and select a schedule.
days <SCHED_DAYS>	Schedule object days. Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time <SCHED_TIME_BEGIN>	Schedule object beginning/ending time. Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name <SCHED_NAME>	Schedule object name. Schedule object name. Example: <i>Work Hours</i>
subject <WORD>	Set the health check E-mail subject. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example


```
health-check-email schedule name "Work Hours"
health-check-email address aaa@bbb.com
health-check-email subject "health check email"
health-check-email body "health check notification"
```

Syntax

```
no health-check-email { address | body | schedule | subject }
```

Mode

Log Automation

Description

Clear health check E-mail settings.

Options

address Clear the health check E-mail address.

body Clear the health check E-mail body.

schedule Disable E-mail health check.

subject Clear the health check E-mail subject.

Example

```
no health-check-email schedule
```

Syntax

```
mail-server <HOSTNAME>
```

Mode

Log Automation

Description

Set mail server IP address or hostname.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
mail-server 192.168.168.204
```

Syntax

```
no mail-server
```

Mode

Log Automation

Description

Clear mail server IP address or hostname.

Example

```
no mail-server
```

Syntax

mail-from <EMAIL>

Mode

Log Automation

Description

Set E-mail address to mail from.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

mail-from admin@nsa5000

Syntax

no mail-from

Mode

Log Automation

Description

Clear E-mail address to mail from.

Example

no mail-from

Syntax

authentication-method { { *none* | *pop-before-smtp* } }

Mode

Log Automation

Description

Specify e-mail server authentication method.

Options

none No authentication.

pop-before-smtp Pop before SMTP.

Example

authentication-method pop-before-smtp

Syntax

pop3-server <LOG_POP3_SERVER_NAME>

Mode

Log Automation

Description

POP3 server IP address or hostname.

Options

<LOG_POP3_SERVER_NAME> Log POP3 server name in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
pop3-server 2.2.2.2
```

Syntax

```
no pop3-server
```

Mode

Log Automation

Description

Clear POP3 server IP address or hostname.

Example

```
no pop3-server
```

Syntax

```
pop3-user-name <WORD>
```

Mode

Log Automation

Description

Specify username for authentication.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
pop3-user-name user
```

Syntax

```
no pop3-user-name
```

Mode

Log Automation

Description

Clear specify username for authentication.

Example

```
no pop3-user-name
```

Syntax

```
pop3-password <ENC_PASSWORD>
```

Mode

Log Automation

Description

Specify password for authentication.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
pop3-password 123
```

Syntax

```
no pop3-password
```

Mode

Log Automation

Description

Clear specify password for authentication.

Example

```
no pop3-password
```

Syntax

```
log-action test
```

Mode

Top Level
Config

Description

Check log automation settings.

Example

```
log-action test
```

Syntax

```
mail-server-advanced
```

Mode

Log Automation

Description

Enter mail server advanced mode.

Example

```
mail-server-advanced
```

Syntax

smtp-port <IPv4_PORT>

Mode

Mail Server Advanced

Description

Set E-mail server SMTP TCP port.

Options

<IPv4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

smtp-port 4025

Syntax

connection-security-method { ssl-tls | start-tls }

Mode

Mail Server Advanced

Description

Select a connection security method.

Options

ssl-tls SSL/TLS.

start-tls STARTTLS.

Example

connection-security-method ssl-tls

Syntax

no connection-security-method

Mode

Mail Server Advanced

Description

Disable connection security method.

Example

no connection-security-method

Syntax

smtp-authentication

Mode

Mail Server Advanced

Description

Enable SMTP authentication.

Example

```
smtp-authentication
```

Syntax

```
no smtp-authentication
```

Mode

Mail Server Advanced

Description

Disable SMTP authentication.

Example

```
no smtp-authentication
```

Syntax

```
user-name <WORD>
```

Mode

Mail Server Advanced

Description

Specify username for authentication.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name mailadmin
```

Syntax

```
no user-name
```

Mode

Mail Server Advanced

Description

Clear username for authentication.

Example

```
no user-name
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

Mail Server Advanced

Description

Specify password for authentication.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password mailadmin
```

Syntax

```
no password
```

Mode

Mail Server Advanced

Description

Clear password for authentication.

Example

```
no password
```

Syntax

```
ftp-log
```

Mode

Log Automation

Description

Entering log automation ftp.

Example

```
ftp-log
```

Syntax

```
send-log-to-ftp
```

Mode

FTP Log

Description

Enable send log to ftp.

Example

```
send-log-to-ftp
```

Syntax

```
no send-log-to-ftp
```

Mode

FTP Log

Description

Disable send log to ftp.

Example

```
no send-log-to-ftp
```

Syntax

```
server <IPV4_HOST>
```

Mode

FTP Log

Description

Set ftp server address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
server 3.3.3.3
```

Syntax

```
no server
```

Mode

FTP Log

Description

Clear ftp server address.

Example

```
no server
```

Syntax

```
user-name <WORD>
```

Mode

FTP Log

Description

Set ftp user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name test

Syntax

no user-name

Mode

FTP Log

Description

Clear ftp user name.

Example

no user-name

Syntax

password <ENC_PASSWORD>

Mode

FTP Log

Description

Set ftp password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

password test123

Syntax

no password

Mode

FTP Log

Description

Clear ftp password.

Example

no password

Syntax

directory <WORD>

Mode

FTP Log

Description

Set ftp directory.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

directory logs

Syntax

send-log { { daily hour <UINT8> minute <UINT8> | weekly { fri | mon | sat | sun | thu | tue | wed } hour <UINT8> minute <UINT8> | when-full } }

Mode

FTP Log

Description

Specify when to send log.

Options

- daily*** Daily.
- hour*** Hour.
- <UINT8>*** Integer in the form: D OR 0xHH.
Example: *123*
- minute*** Minute.
- <UINT8>*** Integer in the form: D OR 0xHH.
Example: *123*
- weekly*** Weekly.
- fri*** Friday.
- mon*** Monday.
- sat*** Saturday.
- sun*** Sunday.
- thu*** Thursday.
- tue*** Tuesday.
- wed*** Wednesday.
- hour*** Hour.
- <UINT8>*** Integer in the form: D OR 0xHH.
Example: *123*
- minute*** Minute.
- <UINT8>*** Integer in the form: D OR 0xHH.
Example: *123*
- when-full*** When full.

Example

send-log weekly mon hour 07 minute 30

Syntax

file-format { attachment csv | html | plain-text }

Mode

FTP Log

Description

Specify file format.

Options

attachment Attachment.
csv CSV.

html HTML.

plain-text Plain text.

Example

```
file-format plain-text
```

Syntax

```
include-all-log-information
```

Mode

FTP Log

Description

Include all log information.

Example

```
include-all-log-information
```

Syntax

```
no include-all-log-information
```

Mode

FTP Log

Description

Include default log information.

Example

```
no include-all-log-information
```

Syntax

```
solera
```

Mode

Log Automation

Description

Entering solera capture mode.

Example

```
solera
```

Syntax

solera-capture-stack-integration

Mode

Solera

Description

Enable solera capture stack integration and enter configuration mode.

Example

solera-capture-stack-integration

Syntax

no solera-capture-stack-integration

Mode

Solera

Description

Disable solera capture stack integration.

Example

no solera-capture-stack-integration

Syntax

server { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }

Mode

Solera

Description

Set solera server.

Options

<i>fqdn</i> <ADDR_FQDN>	Set the solera server to fqdn address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i> <ADDR_HOST>	Set the solera server to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_FQDNHOST_ADDR>	Set the solera server as named address object. FQDN/host address object name. Example: <i>Web Server</i>

Example

server host 192.168.168.198

Syntax

no server

Mode

Solera

Description

Clear solera server.

Example

```
no server
```

Syntax

```
protocol { http | https }
```

Mode

Solera

Description

Set solera server protocol.

Options

http HTTP.

https HTTPS.

Example

```
protocol https
```

Syntax

```
port <IPV4_PORT>
```

Mode

Solera

Description

Set solera port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 54443
```

Syntax

```
user <WORD>
```

Mode

Solera

Description

Set solera user.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".

Example: *abc*

Example

```
user mysolerauser
```

Syntax

```
password <ENC_PASSWORD> confirm-password <ENC_PASSWORD>
```

Mode

Solera

Description

Set solera password.

Options

<ENC_PASSWORD>	Password. Example: <i>secret</i>
confirm-password	Confirm solera password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>

Example

```
password mysolerapassword
```

Syntax

```
deepsee-base-url <WORD>
```

Mode

Solera

Description

Set deepsee base URL.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
deepsee-base-url https://$host:$port/ws/pcap?
user=$usr&password=$pwd&method=deepsee&start=$start&stop=$stop&ipproto=$ipproto&srcip=$srcip&dstip=$dstip&srcport=$srcport&dstport=$dstport
```

Syntax

```
pcap-base-url <WORD>
```

Mode

Solera

Description

Set PCAP base URL.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
pcap-base-url https://$host:$port/ws/pcap?
user=$usr&password=$pwd&method=filename&start=$start&stop=$stop&ipproto=$ipproto&srcip=$srcip&dstip=$dstip&srcport=$srcport&dstport=$dstport
```

Syntax

```
link-icon <WORD>
```

Mode

Solera

Description

Set base64-encoded link icon.

Options

```
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
```

Example

```
link-icon data:image/gif;base64,R0lGODlhFAAUAPeYAOXo7+Xo8P7+/vz7/Pv6/Pr5+/39/fz8/eXo8fj4+tHT2ru+yfv7/KfgggIFBAA7
```

Syntax

```
address-to-link { lan | wan }
```

Mode

Solera

Description

Set default zone for address to link from email alerts.

Options

```
lan Default LAN
wan Default WAN
```

Example

```
address-to-link wan
```

Syntax

```
method { dns | dns-then-netbios | netbios | none }
```

Mode

Log Name Resolution

Description

Set name resolution method.

Options

```
dns DNS.
dns-then-netbios DNS then NetBIOS.
```

netbios	NetBIOS.
none	None.

Example

```
method dns
```

Syntax

```
dns { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

Log Name Resolution

Description

Set whether DNS is inherited or set manually with the associated DNS server IP addresses.

Options

inherit	Inherit DNS servers.
static	Set static DNS server
primary	Specify primary DNS server IP address.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
secondary	Specify secondary DNS server IP address.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
tertiary	Specify tertiary DNS server IP address.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
dns primary 192.168.168.165
```

Syntax

```
no dns static { primary | secondary | tertiary }
```

Mode

Log Name Resolution

Description

Manually clear DNS server IP address.

Options

static	Clear static DNS server IP address.
primary	Clear primary DNS server IP address.
secondary	Clear secondary DNS server IP address.
tertiary	Clear tertiary DNS server IP address.

Example

```
no dns primary
```

Syntax

log-action reset-name-cache

Mode

Top Level
Config

Description

Reset Name Cache.

Example

log-action reset-name-cache

Syntax

log-action report-start

Mode

Top Level
Config

Description

Start data collection.

Example

log-action report-start

Syntax

log-action report-stop

Mode

Top Level
Config

Description

Stop data collection.

Example

log-action report-stop

Syntax

report-refresh

Mode

Log Reports

Description

Refresh Report data collection.

Example

report-refresh

Syntax

log-action report-reset

Mode

Top Level
Config

Description

Reset Report data collection.

Example

log-action report-reset

Syntax

report-view { bandwidth-usage-by-ip | bandwidth-usage-by-service | web-site-hits }

Mode

Log Reports

Description

Set reports view.

Options

bandwidth-usage-by-ip Bandwidth usage by IP address.

bandwidth-usage-by-service Bandwidth usage by service.

web-site-hits Web site hits.

Example

report-view web-site-hits

Syntax

show report

Mode

Log Reports

Description

Show log report.

Options

report Show log report.

Example

show report

Syntax

enable

Mode

Viewpoint

Description

Enable viewpoint settings.

Example

enable

Syntax

no enable

Mode

Viewpoint

Description

Disable viewpoint settings.

Example

no enable

Syntax

enable

Mode

Analyzer

Description

Enable analyzer settings.

Example

enable

Syntax

no enable

Mode

Analyzer

Description

Disable analyzer settings.

Example

no enable

Syntax

log aws

Mode

Config

Description

Enter AWS logs configuration mode.

Example

log aws

Syntax

enable

Mode

AWS Logs

Description

Enable logging.

Example

enable

Syntax

no enable

Mode

AWS Logs

Description

Disable logging.

Example

no enable

Syntax

region { canada | frankfurt | ireland | london | mumbai | north-california | north-virginia | ohio | oregon | paris | sao-paulo | seoul | singapore | sydney | tokyo }

Mode

AWS Logs

Description

Set Amazon web services region.

Options

<i>canada</i>	Canada (Central).
<i>frankfurt</i>	EU (Frankfurt).
<i>ireland</i>	EU (Ireland).
<i>london</i>	EU (London).
<i>mumbai</i>	Asia Pacific (Mumbai).
<i>north-california</i>	US West (N. California).

<i>north-virginia</i>	US East (N. Virginia).
<i>ohio</i>	US East (Ohio).
<i>oregon</i>	US West (Oregon).
<i>paris</i>	EU (Paris).
<i>sao-paulo</i>	South America (São Paulo).
<i>seoul</i>	Asia Pacific (Seoul).
<i>singapore</i>	Asia Pacific (Singapore).
<i>sydney</i>	Asia Pacific (Sydney).
<i>tokyo</i>	Asia Pacific (Tokyo).

Example

region london

Syntax

group-name <WORD>

Mode

AWS Logs

Description

Set log group name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

group-name VPN

Syntax

no group-name

Mode

AWS Logs

Description

Clear log group name.

Example

no group-name

Syntax

stream-name <WORD>

Mode

AWS Logs

Description

Set log stream name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
stream-name VPN
```

Syntax

```
no stream-name
```

Mode

AWS Logs

Description

Clear log stream name.

Example

```
no stream-name
```

Syntax

```
synchronization-interval <UINT32>
```

Mode

AWS Logs

Description

Set synchronization interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
synchronization-interval 60
```

Syntax

```
send-log-when-full
```

Mode

AWS Logs

Description

Enable send log when full.

Example

```
send-log-when-full
```

Syntax

```
no send-log-when-full
```

Mode

AWS Logs

Description

Disable send log when full.

Example

```
no send-log-when-full
```

Syntax

```
export sdwan-conn-logs { csv | txt } <UINT32> { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Top Level
Config

Description

Export sdwan connection logs.

Options

csv	CSV format.
txt	Text format.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: userTest@10.10.10.10:/home/userTest/
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: 80

Example

```
export sdwan-conn-logs csv 1000 scp user@server:/home/user/filename.csv
export sdwan-conn-logs csv 1000 ftp ftp://user@server:/home/user/filename.csv
export sdwan-conn-logs csv 1000 api
```

Syntax

```
log audit
```

Mode

Config

Description

Enter audit configuration mode.

Example

log audit

Syntax

enable

Mode

Configuration Audit

Description

Enable configuration audit.

Example

enable

Syntax

no enable

Mode

Configuration Audit

Description

Disable configuration audit.

Example

no enable

Syntax

display-on-console

Mode

Configuration Audit

Description

Show configuration auditing records to console.

Example

display-on-console

Syntax

no display-on-console

Mode

Configuration Audit

Description

Disable console output of auditing records.

Example

no display-on-console

Syntax

supplemental-changes

Mode

Configuration Audit

Description

Enable configuration audit for supplemental parameter changes.

Example

supplemental-changes

Syntax

no supplemental-changes

Mode

Configuration Audit

Description

Disable configuration audit for supplemental parameter changes.

Example

no supplemental-changes

Syntax

email audit

Mode

Top Level
Config

Description

E-mail audit records now.

Example

email audit

Syntax

export audit { csv | txt } { api | ftp <FTP_URL> | scp <SCP_URL> [port <IPV4_PORT>] }

Mode

Top Level
Config

Description

Export auditing records in csv or txt format.

Options

csv CSV format.

txt Text format.

api	Export using the api.
ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export audit csv ftp ftp://user:password@servername/
export audit csv user@server/
export audit csv scp scp://user@server/
```

Syntax

```
show log [ analyzer [ [ base | syslog-servers ] ] | audit [ [ settings | view ] ] | automation | aws [ [ status ] ] |
categories [ [ attributes [ [ categories | category <LOG_CATEGORY_NAME> [ group <LOG_GROUP_NAME> [ event <LOG_EVENT_NAME> ] ]
| event <LOG_EVENT_ID> | events | group <LOG_GROUP_ID> | groups ] ] | global-category-attributes | statistics [ category-level
<LOG_CATEGORY_BRANCH_LEVEL> ] [ id <INT32> ] [ name <WORD> ] ] ] | display | name-resolution | syslog [ [ base | syslog-server
<SYSLOG_SERVER> port <SYSLOG_SERVER_PORT> profile <SYSLOG_SERVER_PROFILE> | syslog-servers ] ] | view [ { [ { [ id
<LOG_EVENT_ID> ] [ category <LOG_CATEGORY_NAME> ] [ priority <WORD> ] [ source-interface <LOG_INTERFACE_NAME> ] [ destination-
interface <LOG_INTERFACE_NAME> ] [ source-ip <IP_V4V6_HOST> ] [ source-port <UINT16> ] [ destination-ip <IP_V4V6_HOST> ] [
destination-port <UINT16> ] [ ip-protocol <WORD> ] [ user-name <WORD> ] [ application <WORD> ] ] ] | option } ] | view-status
| viewpoint [ [ base | syslog-servers ] ] ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show device log and configuration.

Options

analyzer	Show analyzer settings.
base	Show analyzer base settings.
syslog-servers	Show analyzer syslog server settings.
audit	Show configuration audit.
settings	Show configuration audit settings.
view	View configuration audit messages.
automation	Show log automation settings.
aws	Show AWS logs settings.
status	Show AWS logs status.
categories	Show log categories configuration.
attributes	Show log categories event attributes which have been changed.
categories	Show log attributes for all categories.
category	Show log attributes with specified category name.
<LOG_CATEGORY_NAME>	Log category name. Example: <i>Firewall</i>
group	Show log attributes with specified group name.
<LOG_GROUP_NAME>	Group name. Example: <i>Firewall Event</i>

event	Show log attributes with specified event name.
<LOG_EVENT_NAME>	Event name. Example: <i>Activate Firewall</i>
event	Show log event attributes with specified ID.
<LOG_EVENT_ID>	Event id. Example: <i>200</i>
events	Show log attributes for all events.
group	Show log group attributes with specified ID.
<LOG_GROUP_ID>	Group id. Example: <i>20</i>
groups	Show log attributes for all groups.
global-category-attributes	Show global category attributes.
statistics	Show log categories event statistics.
category-level	Show event statistics of specified category level: category, group or event.
<LOG_CATEGORY_BRANCH_LEVEL>	Log category branch level. Example: <i>Category</i>
id	Show event statistics by event ID.
<INT32>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
name	Show statistics by the name of a category, group or event.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
display	Show time range and max number for showing log view in CLI based current time.
name-resolution	Show name resolution settings.
syslog	Show syslog settings.
base	Show syslog base settings.
syslog-server	Show syslog syslog server settings.
<SYSLOG_SERVER>	Syslog custom server in the form: hostname OR a.b.c.d. Example: <i>abc</i>
port	Log syslog server port.
<SYSLOG_SERVER_PORT>	Syslog custom server port. Example: <i>80</i>
profile	Log syslog server profile.
<SYSLOG_SERVER_PROFILE>	Syslog server profile.
syslog-servers	Show syslog syslog server settings.
view	Show system log.
id	Show log with specified ID.
<LOG_EVENT_ID>	Event id. Example: <i>200</i>
category	Show log with specified category.
<LOG_CATEGORY_NAME>	Log category name. Example: <i>Firewall</i>
priority	Show log with specified priority.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
source-interface	Show log with specified source interface.
<LOG_INTERFACE_NAME>	Interface name. Example: <i>X0</i>
destination-interface	Show log with specified destination interface.
<LOG_INTERFACE_NAME>	Interface name. Example: <i>X0</i>
source-ip	Show log with specified source-ip.
<IP_V4V6_HOST>	IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
source-port	Show log with specified source-port.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

<i>destination-ip</i> <IP_V4V6_HOST>	Show log with specified destination-ip. IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652</i>
<i>destination-port</i> <UINT16>	Show log with specified destination-port. Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>ip-protocol</i> <WORD>	Show log with specified IP protocol. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>user-name</i> <WORD>	Show log with specified user name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>application</i> <WORD>	Show log with specified application. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>option</i>	Show log with specified option.
<i>view-status</i>	Show system log status.
<i>viewpoint</i>	Show viewpoint settings.
<i>base</i>	Show viewpoint base settings.
<i>syslog-servers</i>	Show viewpoint syslog server settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show log
show log view
show log categories
show log categories statistics category-level Category
show log syslog
show log audit view
show log audit settings
```

Syntax

```
voip
```

Mode

Config

Description

Enter VoIP configuration mode.

Example

```
voip
```

Syntax

```
flush-all
```

Mode

VoIP

Description

Flush all VoIP call entry.

Example

flush-all

Syntax

consistent-nat

Mode

VoIP

Description

Enable consistent nat.

Example

consistent-nat

Syntax

no consistent-nat

Mode

VoIP

Description

Disable consistent nat.

Example

no consistent-nat

Syntax

sip

Mode

VoIP

Description

Enter SIP transformations configure mode.

Example

sip

Syntax

enable

Mode

SIP

Description

Enable SIP transformations.

Example

enable

Syntax

no enable

Mode

SIP

Description

Disable SIP transformations.

Example

no enable

Syntax

h323

Mode

VoIP

Description

Enter H.323 transformations configure mode.

Example

h323

Syntax

enable

Mode

H323

Description

Enable H.323 transformations.

Example

enable

Syntax

no enable

Mode

H323

Description

Disable H.323 transformations.

Example

no enable

Syntax

access-rule-based

Mode

SIP

Description

Set SIP transformation will be performed only when it is enabled on the corresponding firewall access rule.

Example

```
access-rule-based
```

Syntax

```
no access-rule-based
```

Mode

SIP

Description

Set SIP transformation will be performed for all SIP sessions on the firewall.

Example

```
no access-rule-based
```

Syntax

```
tcp
```

Mode

SIP

Description

Enable transformations on TCP connections.

Example

```
tcp
```

Syntax

```
no tcp
```

Mode

SIP

Description

Disable transformations on TCP connections.

Example

```
no tcp
```

Syntax

```
transforms-in-service-object { group <SVC_GROUP_NAME> | name <SVC_NAME> }
```

Mode

SIP

Description

Enable transformations for TCP/UDP port(s) in service object.

Options

<i>group</i>	Service group name.
<i><SVC_GROUP_NAME></i>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<i><SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>

Example

```
transforms-in-service-object name Ping
```

Syntax

```
no transforms-in-service-object
```

Mode

SIP

Description

Clear transformations for TCP/UDP port(s) in service object.

Example

```
no transforms-in-service-object
```

Syntax

```
non-sip-packets
```

Mode

SIP

Description

Enable permit non-SIP packets on signaling port.

Example

```
non-sip-packets
```

Syntax

```
no non-sip-packets
```

Mode

SIP

Description

Disable permit non-SIP packets on signaling port.

Example

```
no non-sip-packets
```

Syntax

```
b2bua-support
```

Mode

SIP

Description

Enable SIP back-to-back user agent (B2BUA) support.

Example

```
b2bua-support
```

Syntax

```
no b2bua-support
```

Mode

SIP

Description

Disable SIP back-to-back user agent (B2BUA) support.

Example

```
no b2bua-support
```

Syntax

```
signaling-timeout <UINT32>
```

Mode

SIP

Description

Set SIP signaling inactivity time out (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
signaling-timeout 1800
```

Syntax

```
media-timeout <UINT16>
```

Mode

SIP

Description

Set SIP media inactivity time out (seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
media-timeout 120
```

Syntax

```
no signaling-port
```

Mode

SIP

Description

Clear additional SIP signaling port (UDP) for transformations (optional).

Example

```
no signaling-port
```

Syntax

```
signaling-port <UINT16>
```

Mode

SIP

Description

Set additional SIP signaling port (UDP) for transformations (optional).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
signaling-port 45060
```

Syntax

```
endpoint-registration-anomaly-tracking
```

Mode

SIP

Description

Enable SIP endpoint registration anomaly tracking.

Example

```
endpoint-registration-anomaly-tracking
```

Syntax

```
no endpoint-registration-anomaly-tracking
```

Mode

SIP

Description

Disable SIP endpoint registration anomaly tracking.

Example

```
no endpoint-registration-anomaly-tracking
```

Syntax

```
registration-tracking-interval <UINT32>
```

Mode

SIP

Description

Set SIP registration tracking interval (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
registration-tracking-interval 300
```

Syntax

```
failed-registration-threshold <UINT16>
```

Mode

SIP

Description

Set SIP failed registration threshold.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
failed-registration-threshold 5
```

Syntax

```
endpoint-block-interval <UINT16>
```

Mode

SIP

Description

Set endpoint block interval(seconds).

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
endpoint-block-interval 3600
```

Syntax

access-rule-based

Mode

H323

Description

Set H.323 transformation will be performed only when it is enabled on the corresponding firewall access rule.

Example

access-rule-based

Syntax

no access-rule-based

Mode

H323

Description

Set H.323 transformation will be performed for all H.323 sessions on the firewall.

Example

no access-rule-based

Syntax

only-gatekeeper-calls

Mode

H323

Description

Enable only accept incoming calls from gatekeeper.

Example

only-gatekeeper-calls

Syntax

no only-gatekeeper-calls

Mode

H323

Description

Disable only accept incoming calls from gatekeeper.

Example

no only-gatekeeper-calls

Syntax

inactivity-timeout <UINT32>

Mode

H323

Description

Set H.323 signaling/media inactivity time out (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

inactivity-timeout 300

Syntax

no gatekeeper-ip

Mode

H323

Description

Clear default wan/dmz gatekeeper IP address.

Example

no gatekeeper-ip

Syntax

gatekeeper-ip <IPV4_HOST>

Mode

H323

Description

Set default wan/dmz gatekeeper IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

gatekeeper-ip 172.16.10.10

Syntax

show voip [{ pending-config | with-pending-config } | call-status]

Mode

All Modes

Description

Show VoIP status or configuration.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>call-status</i>	Show VoIP call status.

Example

```
show voip
```

Syntax

```
show wwan [ status ]
```

Mode

All Modes

Description

Show WWAN status or configuration.

Options

<i>status</i>	Show WWAN status.

Example

```
show wwan
```

Syntax

```
security-services
```

Mode

Config

Description

Enter security services configuration mode.

Example

```
security-services
```

Syntax

```
synchronize
```

Mode

Security Services

Description

Synchronize licenses with www.mysonicwall.com.

Example

```
synchronize-license
```

Syntax

```
security { maximum | performance-optimized }
```

Mode

Security Services

Description

Set global security services setting.

Options

maximum Use maximum security (recommended).

performance-optimized Use performance optimized.

Example

```
security maximum
```

Syntax

```
reduce-isdn-antivirus-traffic
```

Mode

Security Services

Description

Enable reduce Anti-Virus traffic for ISDN connections.

Example

```
reduce-isdn-antivirus-traffic
```

Syntax

```
no reduce-isdn-antivirus-traffic
```

Mode

Security Services

Description

Disable reduce Anti-Virus traffic for ISDN connections.

Example

```
no reduce-isdn-antivirus-traffic
```

Syntax

```
drop-packets-at-reload
```

Mode

Security Services

Description

Enable drop all packets while IPS, GAV and Anti-Spyware database is reloading.

Example

drop-packets-at-reload

Syntax

no drop-packets-at-reload

Mode

Security Services

Description

Disable drop all packets while IPS, GAV and Anti-Spyware database is reloading.

Example

no drop-packets-at-reload

Syntax

http-clientless-notification-timeout <UINT32>

Mode

Security Services

Description

Set HTTP clientless notification timeout for gateway AntiVirus and AntiSpyware.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

http-clientless-notification-timeout 86400

Syntax

proxy-server

Mode

Security Services

Description

Enter proxy server configure mode.

Example

proxy-server

Syntax

enable

Mode

Security Services Proxy Server

Description

Enable download signature through a proxy server .

Example

enable

Syntax

no enable

Mode

Security Services Proxy Server

Description

Disable download signature through a proxy server .

Example

no enable

Syntax

host <HOSTNAME>

Mode

Security Services Proxy Server

Description

Set hostname or IP address for proxy server.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

host 10.10.10.10

Syntax

no host

Mode

Security Services Proxy Server

Description

Clear hostname or IP address for proxy server.

Example

no host

Syntax

port <IPV4_PORT>

Mode

Security Services Proxy Server

Description

Set proxy server TCP port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 8080
```

Syntax

```
no port
```

Mode

Security Services Proxy Server

Description

Clear proxy server TCP port.

Example

```
no port
```

Syntax

```
authentication { enable | password <ENC_PASSWORD> | user-name <WORD> }
```

Mode

Security Services Proxy Server

Description

Configure proxy server authentication.

Options

enable	Enable proxy server authentication.
password	Set proxy server password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>
user-name	Set proxy server username.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
authentication enable
authentication user-name proxyUser
authentication password proxyPass
```

Syntax

```
no authentication { enable | password | user-name }
```

Mode

Security Services Proxy Server

Description

No configure proxy server authentication.

Options

<i>enable</i>	Enable proxy server authentication.
<i>password</i>	Clear proxy server authentication password.
<i>user-name</i>	Clear proxy server authentication username.

Example

```
no authentication enable
no authentication user-name
no authentication password
```

Syntax

```
portal [ user-name <WORD> ] [ password <ENC_PASSWORD> ]
```

Mode

Security Services Proxy Server

Description

Configure proxy server portal username and password.

Options

<i>user-name</i>	Set proxy server portal username.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>password</i>	Set proxy server portal password.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>

Example

```
portal user-name portalUser
```

Syntax

```
no portal { password | user-name }
```

Mode

Security Services Proxy Server

Description

Clear proxy server portal username or password.

Options

<i>password</i>	Clear proxy server portal password.
<i>user-name</i>	Clear proxy server portal username.

Example

```
no portal user-name
```

Syntax

```
import signature { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Security Services

Description

Import signatures to the firewall.

Options

<i>api</i>	Import using the api.
<i>ftp</i>	Import using the FTP protocol.
<i><FTP_URL></i>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: '.' -> '\\.', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
<i>scp</i>	Import using the SCP protocol.
<i><SCP_URL></i>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
<i>port</i>	SCP server port
<i><IPV4_PORT></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import signature ftp ftp://user:password@servername/xxxx.sig
import signature scp user@server:/home/user/xxxx.sig
```

Syntax

dpi-ssh

Mode

Config

Description

Enter DPI-SSH configuration mode.

Example

dpi-ssh

Syntax

enable

Mode

DPI SSH

Description

Enable SSH inspection.

Example

enable

Syntax

no enable

Mode

DPI SSH

Description

Disable SSH inspection.

Example

```
no enable
```

Syntax

```
intrusion-prevention
```

Mode

DPI SSH

Description

Enable intrusion prevention for DPI-SSH.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

DPI SSH

Description

Disable intrusion prevention for DPI-SSH.

Example

```
no intrusion-prevention
```

Syntax

```
gateway { anti-spyware | anti-virus }
```

Mode

DPI SSH

Description

Enable gateway anti-virus or anti-spyware for DPI-SSH.

Options

anti-spyware Enable gateway anti-spyware for DPI-SSH.

anti-virus Enable gateway anti-virus for DPI-SSH.

Example

```
gateway anti-virus
gateway anti-spyware
```

Syntax

```
no gateway { anti-spyware | anti-virus }
```

Mode

DPI SSH

Description

Disable gateway anti-virus or anti-spyware for DPI-SSH.

Options

anti-spyware Disable gateway anti-spyware for DPI-SSH.

anti-virus Disable gateway anti-virus for DPI-SSH.

Example

```
no gateway anti-virus
no gateway anti-spyware
```

Syntax

```
application-firewall
```

Mode

DPI SSH

Description

Enable application firewall for DPI-SSH.

Example

```
application-firewall
```

Syntax

```
no application-firewall
```

Mode

DPI SSH

Description

Disable application firewall for DPI-SSH.

Example

```
no application-firewall
```

Syntax

```
block-port-forwarding [ global | local | remote | x11 ]
```

Mode

DPI SSH

Description

Block port forwarding.

Options

- global** Block port forwarding.
- local** Block local port forwarding.
- remote** Block remote port forwarding.
- x11** Block X11 forwarding.

Example

```
block-port-forwarding
block-port-forwarding local
block-port-forwarding remote
```

Syntax

```
no block-port-forwarding [ global | local | remote | x11 ]
```

Mode

DPI SSH

Description

Allow port forwarding.

Options

- global** Block port forwarding.
- local** Allow local port forwarding.
- remote** Allow remote port forwarding.
- x11** Allow X11 forwarding.

Example

```
no block-port-forwarding
no block-port-forwarding local
no block-port-forwarding remote
```

Syntax

```
include address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all
| fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion address object or group.

Options

- ipv6** IPv6 address object.
- host** Address object host.
<ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*
- network** Address object network.
<ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: *IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n*

<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
all	All addresses.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
include address name "DPI-SSH Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion address object or group.

Options

ipv6	IPv6 address object.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com.

Example: *example.com*

group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclude address name "DPI-SSH Exclusion Object"
```

Syntax

```
no exclude address
```

Mode

DPI SSH

Description

Clear exclusion address objects or group for DPI-SSH.

Example

```
no exclude address
```

Syntax

```
include service { all | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion service object or group.

Options

all	All services.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
include service name "DPI-SSH Inclusion Service"
```

Syntax

```
exclude service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion service object or group.

Options

group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
exclude service name "DPI-SSH Exclusion Service"
```

Syntax

```
no exclude service
```

Mode

DPI SSH

Description

Clear exclusion service objects or group for DPI-SSH.

Example

```
no exclude service
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

DPI SSH

Description

Set the DPI-SSH inclusion user object or group.

Options

administrator	Administrator.

<i>all</i>	All users.
<i>group</i>	Group object name.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guest users.
<i>name</i>	User object name.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

```
include user group "DPI-SSH User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

DPI SSH

Description

Set the DPI-SSH exclusion user object or group.

Options

<i>administrator</i>	Administrator.
<i>group</i>	Group object name.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guest users.
<i>name</i>	User object name.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

```
exclude user group "DPI-SSH User Group"
```

Syntax

```
no exclude user
```

Mode

DPI SSH

Description

Clear exclusion user for DPI-SSH.

Example

```
no exclude user
```

Syntax

```
content-filter
```

Mode

Config

Description

Enter content filter configuration mode.

Example

```
content-filter
```

Syntax

```
filter-type { cfs | websense }
```

Mode

Content Filter

Description

Set filter type and enter corresponding configuration mode.

Options

cfs SonicWall CFS.

websense Websense enterprise.

Example

```
filter-type cfs
filter-type websense
```

Syntax

```
cfs
```

Mode

Content Filter

Description

Enter CFS configuration mode.

Example

```
cfs
```

Syntax

```
websense
```

Mode

Content Filter

Description

Enter Websense configuration mode.

Example

```
websense
```

Syntax

max-url-caches <UINT32>

Mode

SonicWall CFS

Description

Set CFS max URL caches number.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

max-url-caches 51200

Syntax

enable

Mode

SonicWall CFS

Description

Enable CFS.

Example

enable

Syntax

no enable

Mode

SonicWall CFS

Description

Disable CFS.

Example

no enable

Syntax

block-if-server-unavailable

Mode

SonicWall CFS

Description

Enable block if CFS server is unavailable.

Example

block-if-server-unavailable

Syntax

```
no block-if-server-unavailable
```

Mode

SonicWall CFS

Description

Disable block if CFS server is unavailable.

Example

```
no block-if-server-unavailable
```

Syntax

```
server-timeout <UINT16>
```

Mode

SonicWall CFS

Description

Set CFS server timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
server-timeout 5
```

Syntax

```
local-server { enable | primary <HOSTNAME_MIXED> | secondary <HOSTNAME_MIXED> }
```

Mode

SonicWall CFS

Description

Enable local CFS server and set address.

Options

- enable** Disable local CFS server.
- primary** Set primary local CFS server.
<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n
- secondary** Set secondary local CFS server.
<HOSTNAME_MIXED> IPV4: hostname in the form: D.D.D.D or hostname\nIPV6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652\n

Example

```
local-server enable
local-server primary 1.1.1.1
local-server secondary localserver.sonicwall.com
```

Syntax

```
no local-server { enable | primary | secondary }
```

Mode

SonicWall CFS

Description

Disable local CFS server or clear server address.

Options

enable Disable local CFS server.

primary Clear primary local CFS server.

secondary Clear secondary local CFS server.

Example

```
no local-server enable
no local-server primary
no local-server secondary
```

Syntax

```
exclude administrator
```

Mode

SonicWall CFS

Description

Enable exclude administrator.

Example

```
exclude administrator
```

Syntax

```
no exclude administrator
```

Mode

SonicWall CFS

Description

Diablo exclude administrator.

Example

```
no exclude administrator
```

Syntax

```
exclude address { { [ ipv6 ] { fqdn <ADDR_FQDN> | host <ADDR_HOST> | mac <ADDR_MAC> | network <ADDR_NETWORK> <ADDR_MASK> |
range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

SonicWall CFS

Description

Exclude address.

Options

ipv6	IPv6 Address object.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Address object MAC Address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
network <ADDR_NETWORK> <ADDR_MASK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN> <ADDR_END>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Address object group name. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

```
exclude address host 192.168.168.168
exclude address network 192.168.168.0 255.255.255.0
exclude address range 192.168.168.1 192.168.168.10
exclude address mac D067E534E99C
exclude address fqdn example.com
exclude address ipv6 host fec0:1::1
exclude address ipv6 network fec0:1:: 64
exclude address ipv6 range fec0:1::1 fec0:1::100
exclude address group "Corp CFS Exclusion Address Group"
exclude address name "Corp CFS Exclusion Address Object"
```

Syntax

```
no exclude address
```

Mode

SonicWall CFS

Description

Clear excluded address.

Example

```
no exclude address
```


Syntax

```
clear policies statistics
```

Mode

SonicWall CFS

Description

Clear all statistics of CFS policies.

Options

statistics Clear all statistics of CFS policies.

Example

```
clear policies statistics
```

Syntax

```
clear policy <CFS_POLICY_NAME> statistics
```

Mode

SonicWall CFS

Description

Clear statistics of specified CFS policy.

Options

<CFS_POLICY_NAME> CFS policy name.
Example: *Market policy*

statistics Clear statistics of specified CFS policy.

Example

```
clear policy "CFS Default profile" statistics
```

Syntax

```
no policies
```

Mode

SonicWall CFS

Description

Delete all CFS policies.

Example

```
no policies
```

Syntax

```
no policy [ uuid ] <CFS_POLICY_NAME>
```

Mode

SonicWall CFS

Description

Delete CFS policy.

Options

- uuid** Delete CFS policy by UUID.
- <CFS_POLICY_NAME>** CFS policy name.
Example: *Market policy*

Example

no policy "policyName"

Syntax

policy [uuid] <CFS_POLICY_NAME>

Mode

SonicWall CFS

Description

Add/Edit CFS policy and enter configuration mode.

Options

- uuid** Select CFS policy by UUID.
- <CFS_POLICY_NAME>** CFS policy name.
Example: *Market policy*

Example

policy "CFS default policy"

Syntax

uuid <UUID>

Mode

CFS Policy

Description

Set Policy Uuid.

Options

- <UUID>** Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid "374099bb-47a2-dc7e-1100-c0eae49ce84c"

Syntax

no uuid

Mode

CFS Policy

Description

Delete Policy by Uuid.

Example

uuid "374099bb-47a2-dc7e-1100-c0eae49ce84c"

Syntax

name <CFS_POLICY_NAME>

Mode

CFS Policy

Description

Set policy name.

Options

<CFS_POLICY_NAME> CFS policy name.
Example: *Market policy*

Example

name "CFS default policy"

Syntax

source zone <CFS_POLICY_ZONE>

Mode

CFS Policy

Description

Set source zone.

Options

<CFS_POLICY_ZONE> CFS policy zone.
Example: *LAN*

Example

source zone LAN

Syntax

destination zone <CFS_POLICY_ZONE>

Mode

CFS Policy

Description

Set destination zone.

Options

<CFS_POLICY_ZONE> CFS policy zone.
Example: *LAN*

Example

destination zone WAN

Syntax

```
source address included { { [ ipv6 ] { host <CFS_POLICY_ADDR_HOST> | network <CFS_POLICY_ADDR_NETWORK> <CFS_POLICY_ADDR_MASK>
| range <CFS_POLICY_ADDR_BEGIN> <CFS_POLICY_ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac
<ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

CFS Policy

Description

Set included source address.

Options

ipv6	IPv6 Address object.
host <CFS_POLICY_ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <CFS_POLICY_ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<CFS_POLICY_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <CFS_POLICY_ADDR_BEGIN>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<CFS_POLICY_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group object name. Group address object name. Example: <i>Sales Group</i>
mac <ADDR_MAC>	Address object MAC Address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

```
source address included host 192.168.168.168
source address included network 192.168.168.0 255.255.255.0
source address included range 192.168.168.1 192.168.168.10
source address included mac D067E534E99C
source address included fqdn example.com
source address included ipv6 host fec0:1::1
source address included ipv6 network fec0:1::: 64
source address included ipv6 range fec0:1::1 fec0:1::100
source address included any
source address included group "CFS Policy Source Address Group"
source address included name "CFS Policy Source Address Object"
```

Syntax

```
source address excluded { { [ ipv6 ] { host <CFS_POLICY_ADDR_HOST> | network <CFS_POLICY_ADDR_NETWORK> <CFS_POLICY_ADDR_MASK>
| range <CFS_POLICY_ADDR_BEGIN> <CFS_POLICY_ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC>
| name <ADDR_NAME_MIXED> | none }
```

Mode

Description

Set excluded source address.

Options

<i>ipv6</i>	IPv6 Address object.
<i>host</i>	Address object host.
<i><CFS_POLICY_ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i>	Address object network.
<i><CFS_POLICY_ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><CFS_POLICY_ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Specify IP range.
<i><CFS_POLICY_ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><CFS_POLICY_ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>fqdn</i>	Address object full qualified domain name.
<i><ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i>	Address group object name.
<i><ADDR_GROUP_NAME_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>mac</i>	Address object MAC Address.
<i><ADDR_MAC></i>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i>	Address object name.
<i><ADDR_NAME_MIXED></i>	Address object name. Example: <i>Web Server</i>
<i>none</i>	None address.

Example

```
source address excluded host 192.168.168.168
source address excluded network 192.168.168.0 255.255.255.0
source address excluded range 192.168.168.1 192.168.168.10
source address excluded mac D067E534E99C
source address excluded fqdn example.com
source address excluded ipv6 host fec0:1::1
source address excluded ipv6 network fec0:1:: 64
source address excluded ipv6 range fec0:1::1 fec0:1::100
source address excluded none
source address excluded group "CFS Policy Source Address Group"
source address excluded name "CFS Policy Source Address Object"
```

Syntax

```
user included { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Description

Set included users.

Options

administrator	Administrator.
all	All users.
group	User group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests.
name	User object name.
<LOCAL_USER_NAME>	Local user object name. Example: <i>user1</i>

Example

```
user included all
user included guests
user included administrator
user included name "user1"
user included group "Limited Administrators"
```

Syntax

```
user excluded { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> | none }
```

Mode

CFS Policy

Description

Set excluded users.

Options

administrator	Administrator.
group	User group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests.
name	User object name.
<LOCAL_USER_NAME>	Local user object name. Example: <i>user1</i>
none	None users.

Example

```
user excluded none
user excluded guests
user excluded administrator
user excluded name "user1"
user excluded group "Limited Administrators"
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

CFS Policy

Description

Set schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule always-on
schedule name "Schedule Name"
schedule days "Schedule Days" time "Schedule Time Begin" "Schedule Time End"
```

Syntax

```
profile <CONTENT_FILTER_PROFILE_NAME>
```

Mode

CFS Policy

Description

Set profile.

Options

<i><CONTENT_FILTER_PROFILE_NAME></i>	Content filter profile object name. Example: <i>Market profile</i>

Example

```
profile "CFS Default profile"
```

Syntax

```
action <CONTENT_FILTER_ACTION_NAME>
```

Mode

CFS Policy

Description

Set action.

Options

<i><CONTENT_FILTER_ACTION_NAME></i>	Content filter action object name. Example: <i>Market action</i>

Example

```
action "CFS Default action"
```

Syntax

enable

Mode

CFS Policy

Description

Enable the policy.

Example

enable

Syntax

no enable

Mode

CFS Policy

Description

Disable the policy.

Example

no enable

Syntax

priority <UINT32>

Mode

CFS Policy

Description

Set priority.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

priority 3

Syntax

no priority

Mode

CFS Policy

Description

Clear priority.

Example

no priority

Syntax

```
import custom-category { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

SonicWall CFS

Description

Import content filter CFS custom category data.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: '.' -> '\\.', '@' -> '\\@', ' ' -> '\\\\', '\\ ' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/nftp://username@hostname/nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import custom-category ftp ftp://user:password@servername/cfsCustomCategoryData.wri
import custom-category scp user@server:/home/user/cfsCustomCategoryData.wri
```

Syntax

```
custom-category
```

Mode

SonicWall CFS

Description

Enter CFS custom category configuration mode.

Example

```
custom-category
```

Syntax

```
enable
```

Mode

CFS Custom Category

Description

Enable custom category.

Example

```
enable
```

Syntax

```
no enable
```

Mode

CFS Custom Category

Description

Disable custom category.

Example

```
no enable
```

Syntax

```
no category-entries
```

Mode

CFS Custom Category

Description

Delete all custom category entries.

Example

```
no category-entries
```

Syntax

```
no category-entry <CFS_CUSTOM_CATEGORY_DOMAIN>
```

Mode

CFS Custom Category

Description

Delete custom category entry.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

```
no category-entry yahoo.com
```

Syntax

```
category-entry <CFS_CUSTOM_CATEGORY_DOMAIN>
```

Mode

CFS Custom Category

Description

Add/Edit custom category entry and enter configuration mode.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

```
category-entry www.google.com
```

Syntax

domain <CFS_CUSTOM_CATEGORY_DOMAIN>

Mode

Content Filter Custom Category Entry

Description

Set custom category entry domain.

Options

<CFS_CUSTOM_CATEGORY_DOMAIN> CFS custom category domain.
Example: *google.com*

Example

domain www.google.com

Syntax

no ratings

Mode

Content Filter Custom Category Entry

Description

Delete all ratings of category entry.

Example

no ratings

Syntax

rating <CONTENT_FILTER_CATEGORY_ID_NAME>

Mode

Content Filter Custom Category Entry

Description

Add rating for category entry.

Options

<CONTENT_FILTER_CATEGORY_ID_NAME> Content filter category number and name.
Example: *1. Violence/Hate/Racism*

Example

rating "1.Violence/Hate/Racism"

Syntax

no rating <CFS_CUSTOM_CATEGORY_RATING>

Mode

Content Filter Custom Category Entry

Description

Delete rating of category entry.

Options

<CFS_CUSTOM_CATEGORY_RATING> CFS custom category rating number and name.
Example: *1. Violence/Hate/Racism*

Example

```
no rating "1.Violence/Hate/Racism"
```

Syntax

```
synchronize local-server-info
```

Mode

SonicWall CFS

Description

Get latest local server info.

Example

```
synchronize local-server-info
```

Syntax

```
no uri-list-objects
```

Mode

Content Filter

Description

Delete all content filter URI list objects.

Example

```
no uri-list-objects
```

Syntax

```
no uri-list-groups
```

Mode

Content Filter

Description

Delete all content filter URI list groups.

Example

```
no uri-list-groups
```

Syntax

```
no uri-list-object [ uuid ] <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter

Description

Delete content filter URI list object.

Options

<i>uuid</i>	Select URL object by UUID.
<i><CONTENT_FILTER_URI_LIST_OBJ_NAME></i>	Content filter URI list object name. Example: <i>White URI list object</i>

Example

no uri-list-object "uriListObjName"

Syntax

no uri-list-group [uuid] <CONTENT_FILTER_URI_LIST_GRP_NAME>

Mode

Content Filter

Description

Delete content filter URI list group.

Options

<i>uuid</i>	Select URL object by UUID.
<i><CONTENT_FILTER_URI_LIST_GRP_NAME></i>	Content filter URI list group name. Example: <i>White URI list group</i>

Example

no uri-list-group "uriListGrpName"

Syntax

uri-list-object [uuid] <CONTENT_FILTER_URI_LIST_OBJ_NAME>

Mode

Content Filter

Description

Add/Edit content filter URI list object and enter configuration mode.

Options

<i>uuid</i>	Select URL object by UUID.
<i><CONTENT_FILTER_URI_LIST_OBJ_NAME></i>	Content filter URI list object name. Example: <i>White URI list object</i>

Example

uri-list-object "Uri List Object Name"

Syntax

uri-list-group [uuid] <CONTENT_FILTER_URI_LIST_GRP_NAME>

Mode

Content Filter

Description

Add/Edit content filter URI list group and enter configuration mode.

Options

<code>uuid</code>	Select URL object by UUID.
<code><CONTENT_FILTER_URI_LIST_GRP_NAME></code>	Content filter URI list group name. Example: <i>White URI list group</i>

Example

`uri-list-group "Uri List Group Name"`

Syntax

`name <CONTENT_FILTER_URI_LIST_OBJ_NAME>`

Mode

Content Filter URI List Object

Description

Set URI list object name.

Options

<code><CONTENT_FILTER_URI_LIST_OBJ_NAME></code>	Content filter URI list object name. Example: <i>White URI list object</i>

Example

`name "default URI List"`

Syntax

`name <CONTENT_FILTER_URI_LIST_GRP_NAME>`

Mode

Content Filter URI List Group

Description

Set URI list group name.

Options

<code><CONTENT_FILTER_URI_LIST_GRP_NAME></code>	Content filter URI list group name. Example: <i>White URI list group</i>

Example

`name "default URI List"`

Syntax

`type <CONTENT_FILTER_URI_LIST_OBJ_TYPE>`

Mode

Content Filter URI List Object

Description

Set URI list object type.

Options

<code><CONTENT_FILTER_URI_LIST_OBJ_TYPE></code>	Content filter URI list object type.

Example: *domain*

Example

```
type uri/domain/keyword
```

Syntax

```
no entries
```

Mode

Content Filter URI List Object

Description

Remove all entries from URI list.

Example

```
no entries
```

Syntax

```
no uri-list-group-members
```

Mode

Content Filter URI List Group

Description

Remove all members from uri-list-group.

Example

```
no uri-list-group-members
```

Syntax

```
uri <CONTENT_FILTER_URI_LIST_ENTRY>
```

Mode

Content Filter URI List Object

Description

Add URI into URI list object.

Options

<CONTENT_FILTER_URI_LIST_ENTRY>	Content filter URI list entry. Example: <i>google.com</i>

Example

```
uri www.google.com
```

Syntax

```
no uri <CONTENT_FILTER_URI_LIST_ENTRY>
```

Mode

Content Filter URI List Object

Description

Remove URI from URI list.

Options

<CONTENT_FILTER_URI_LIST_ENTRY> Content filter URI list entry.
Example: *google.com*

Example

no uri www.google.com

Syntax

no uris

Mode

Content Filter URI List Object

Description

Remove all URIs from URI list.

Example

no uris

Syntax

keyword <CONTENT_FILTER_URI_LIST_ENTRY>

Mode

Content Filter URI List Object

Description

Add keyword into URI list.

Options

<CONTENT_FILTER_URI_LIST_ENTRY> Content filter URI list entry.
Example: *google.com*

Example

keyword news

Syntax

no keyword <CONTENT_FILTER_URI_LIST_ENTRY>

Mode

Content Filter URI List Object

Description

Remove keyword from URI list.

Options

<CONTENT_FILTER_URI_LIST_ENTRY> Content filter URI list entry.
Example: *google.com*

Example

no keyword news

Syntax

no keywords

Mode

Content Filter URI List Object

Description

Remove all keywords from URI list.

Example

no keywords

Syntax

domain <CONTENT_FILTER_URI_LIST_ENTRY>

Mode

Content Filter URI List Object

Description

Add domain into URI list.

Options

<CONTENT_FILTER_URI_LIST_ENTRY> Content filter URI list entry.
Example: *google.com*

Example

domain yahoo.com

Syntax

no domain <CONTENT_FILTER_URI_LIST_ENTRY>

Mode

Content Filter URI List Object

Description

Remove domain from URI list.

Options

<CONTENT_FILTER_URI_LIST_ENTRY> Content filter URI list entry.
Example: *google.com*

Example

no domain news

Syntax

no domains

Mode

Content Filter URI List Object

Description

Remove all domains from URI list.

Example

```
no domains
```

Syntax

```
location <WORD>
```

Mode

Content Filter URI List Object

Description

Set Location address of dynamic list.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
location http://1.1.1.1/blacklist.txt
```

Syntax

```
no location
```

Mode

Content Filter URI List Object

Description

Clear location address of dynamic list.

Example

```
no location
```

Syntax

```
exclusion <CONTENT_FILTER_URI_LIST_DOMAIN_NAME>
```

Mode

Content Filter URI List Object

Description

Set exclusion list of dynamic list.

Options

<CONTENT_FILTER_URI_LIST_DOMAIN_NAME> Content filter URI list object (Domain) name.
Example: *White Domain list object*

Example

```
exclusion allowed-list
```

Syntax

no exclusion

Mode

Content Filter URI List Object

Description

Clear exclusion list of dynamic list.

Example

no exclusion

Syntax

auto-sync

Mode

Content Filter URI List Object

Description

Enable auto sync of dynamic list.

Example

auto-sync

Syntax

no auto-sync

Mode

Content Filter URI List Object

Description

Disable auto sync of dynamic list.

Example

no auto-sync

Syntax

sync-interval <UINT32>

Mode

Content Filter URI List Object

Description

Set sync interval of dynamic list.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

sync-interval 2

Syntax

```
no sync-interval
```

Mode

Content Filter URI List Object

Description

Clear sync interval of dynamic list.

Example

```
no sync-interval
```

Syntax

```
export uris { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Content Filter URI List Object

Config

Description

Download uri expressions.

Options

ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>

Example

```
export uris ftp ftp://user:password@servername/customizedUriList.rtf
export uris scp scp://user@server/customizedUriList.rtf
```

Syntax

```
import uris { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPv4_PORT> ] }
```

Mode

Content Filter URI List Object

Description

Upload uri expressions.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPv4_PORT>	Integer in the form: D OR 0xHHHH.

Example

```
import uris ftp ftp://user:password@servername/customizedUriList.rtf
import uris scp scp://user@server/customizedUriList.rtf
```

Syntax

```
export keywords { ftp <FTP_URL> | scp <SCP_URL> }
```

Mode

Content Filter URI List Object
Config

Description

Download keywords.

Options

ftp Export using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: `ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/`

scp Export using the SCP protocol.

<SCP_URL> SCP URL in the form: userName@serverip:/fileDirectory.
Example: `userTest@10.10.10.10:/home/userTest/`

Example

```
export keyword ftp ftp://user:password@servername/customizedKeywordList.rtf
export keyword scp scp://user@server/customizedKeywordList.rtf
```

Syntax

```
import keywords { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Content Filter URI List Object

Description

Upload keywords.

Options

api Import using the api.

ftp Import using the FTP protocol.

<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: `ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/`

scp Import using the SCP protocol.

<SCP_URL> SCP URL in the form: userName@serverip:/fileDirectory.
Example: `userTest@10.10.10.10:/home/userTest/`

port SCP server port

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
import keyword ftp ftp://user:password@servername/customizedKeywordList.rtf
import keyword scp scp://user@server/customizedKeywordList.rtf
```

Syntax

```
uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter URI List Group

Description

Assign URI list object to group.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
uri-list-object "allowed uri list object"
```

Syntax

```
no uri-list-object <CONTENT_FILTER_URI_LIST_OBJ_NAME>
```

Mode

Content Filter URI List Group

Description

Remove URI list object from group.

Options

<CONTENT_FILTER_URI_LIST_OBJ_NAME> Content filter URI list object name.
Example: *White URI list object*

Example

```
no uri-list-object "white list object"
```

Syntax

```
uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Content Filter URI List Group

Description

Assign URI list group to group.

Options

<CONTENT_FILTER_URI_LIST_GRP_NAME> Content filter URI list group name.
Example: *White URI list group*

Example

```
uri-list-group "white list group"
```

Syntax

```
no uri-list-group <CONTENT_FILTER_URI_LIST_GRP_NAME>
```

Mode

Description

Remove URI list group from group.

Options

`<CONTENT_FILTER_URI_LIST_GRP_NAME>` Content filter URI list group name.
Example: *White URI list group*

Example

`no uri-list-group "white list group"`

Syntax

`no actions`

Mode

Content Filter

Description

Delete all content filter action objects.

Example

`no actions`

Syntax

`no action [ uuid ] <CONTENT_FILTER_ACTION_NAME>`

Mode

Content Filter

Description

Delete content filter action object.

Options

`uuid` Select CFS action object by UUID.
`<CONTENT_FILTER_ACTION_NAME>` Content filter action object name.
Example: *Market action*

Example

`no action "actionName"`

Syntax

`action [ uuid ] <CONTENT_FILTER_ACTION_NAME>`

Mode

Content Filter

Description

Add/Edit content filter action object and enter configuration mode.

Options

`uuid` Select CFS action object by UUID.
`<CONTENT_FILTER_ACTION_NAME>` Content filter action object name.

Example: *Market action*

Example

```
action "actionName"
```

Syntax

```
name <CONTENT_FILTER_ACTION_NAME>
```

Mode

Content Filter Action Object

Description

Set action object name.

Options

<CONTENT_FILTER_ACTION_NAME> Content filter action object name.
Example: *Market action*

Example

```
name "actionName"
```

Syntax

```
wipe-cookies
```

Mode

Content Filter Action Object

Description

Enable wipe cookies.

Example

```
wipe-cookies
```

Syntax

```
no wipe-cookies
```

Mode

Content Filter Action Object

Description

Disable wipe cookies.

Example

```
no wipe-cookies
```

Syntax

```
flow-reporting
```

Mode

Content Filter Action Object

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Content Filter Action Object

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

block page { custom <WORD> | default }

Mode

Content Filter Action Object

Description

Set block page.

Options

- custom*** Use custom defined page.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default*** Use default page.

Example

block page custom "<html> ... </html>"
block page default

Syntax

passphrase page { custom <WORD> | default }

Mode

Content Filter Action Object

Description

Set passphrase page.

Options

- custom*** Use custom defined page.
- <WORD>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

default Use default page.

Example

```
passphrase page custom "<html> ... </html>"
passphrase page default
```

Syntax

```
passphrase password <ENC_PASSWORD>
```

Mode

Content Filter Action Object

Description

Set passphrase password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
passphrase password 123456
```

Syntax

```
no passphrase password
```

Mode

Content Filter Action Object

Description

Clear passphrase password.

Example

```
no passphrase password
```

Syntax

```
passphrase active-time <UINT32>
```

Mode

Content Filter Action Object

Description

Set passphrase active time.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
passphrase active-time 60
```

Syntax

```
confirm page { custom <WORD> | default }
```

Mode

Content Filter Action Object

Description

Set confirm page.

Options

- custom** Use custom defined page.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default** Use default page.

Example

```
confirm page custom "<html> ... </html>"
confirm page default
```

Syntax

```
confirm active-time <UINT32>
```

Mode

Content Filter Action Object

Description

Set confirm active time.

Options

- <UINT32>** Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
confirm active-time 60
```

Syntax

```
bandwidth-management aggregation-method { action | policy }
```

Mode

Content Filter Action Object

Description

Set bandwidth management aggregation method.

Options

- action** Use per action aggregation method.
- policy** Use per policy aggregation method.

Example

```
bandwidth-management aggregation-method policy
```

Syntax

```
bandwidth-management egress [ name <BANDWIDTH_RULE_NAME> ]
```

Mode

Content Filter Action Object

Description

Enable egress bandwidth management or set egress object.

Options

name	Set egress bandwidth management object.
<BANDWIDTH_RULE_NAME>	Bandwidth object name. Example: <code>\ "Corp High Priority\"</code>

Example

```
bandwidth-management egress
bandwidth-management egress name "Egress BWM Object"
```

Syntax

```
no bandwidth-management egress [ name ]
```

Mode

Content Filter Action Object

Description

Disable egress bandwidth management or clear egress object.

Options

name	Clear egress bandwidth management object.

Example

```
no bandwidth-management egress
no bandwidth-management egress name
```

Syntax

```
bandwidth-management ingress [ name <BANDWIDTH_RULE_NAME> ]
```

Mode

Content Filter Action Object

Description

Enable ingress bandwidth management or set ingress object.

Options

name	Set ingress bandwidth management object.
<BANDWIDTH_RULE_NAME>	Bandwidth object name. Example: <code>\ "Corp High Priority\"</code>

Example

```
bandwidth-management ingress
bandwidth-management ingress name "Ingress BWM Object"
```

Syntax

```
no bandwidth-management ingress [ name ]
```

Mode

Content Filter Action Object

Description

Disable ingress bandwidth management or clear ingress object.

Options

name Clear ingress bandwidth management object.

Example

```
no bandwidth-management ingress
no bandwidth-management ingress name
```

Syntax

```
bandwidth-management usage-tracking
```

Mode

Content Filter Action Object

Description

Enable bandwidth usage tracking.

Example

```
bandwidth-management usage-tracking
```

Syntax

```
no bandwidth-management usage-tracking
```

Mode

Content Filter Action Object

Description

Disable bandwidth usage tracking.

Example

```
no bandwidth-management usage-tracking
```

Syntax

```
no profiles
```

Mode

Content Filter

Description

Delete all content filter profile objects.

Example

```
no profiles
```

Syntax

```
no profile [ uuid ] <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter

Description

Delete content filter profile object.

Options

uuid	Delete CFS profile object by UUID.
<CONTENT_FILTER_PROFILE_NAME>	Content filter profile object name. Example: <i>Market profile</i>

Example

```
no profile profileName
```

Syntax

```
profile [ uuid ] <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter

Description

Add/Edit content filter profile object and enter configuration mode.

Options

uuid	Select CFS profile object by UUID.
<CONTENT_FILTER_PROFILE_NAME>	Content filter profile object name. Example: <i>Market profile</i>

Example

```
profile profileName
```

Syntax

```
name <CONTENT_FILTER_PROFILE_NAME>
```

Mode

Content Filter Profile Object

Description

Set profile object name.

Options

<CONTENT_FILTER_PROFILE_NAME>	Content filter profile object name. Example: <i>Market profile</i>

Example

```
name profileName
```

Syntax

```
uri-list allowed <CONTENT_FILTER_URI_LIST_NAME>
```

Mode

Content Filter Profile Object

Description

Set allowed uri list.

Options

<CONTENT_FILTER_URI_LIST_NAME> Content filter URI list object/group name.
Example: *White URI list*

Example

```
uri-list allowed allowedUriListName
```

Syntax

```
no uri-list allowed
```

Mode

Content Filter Profile Object

Description

Clear allowed uri list.

Example

```
no uri-list allowed
```

Syntax

```
uri-list forbidden <CONTENT_FILTER_URI_LIST_NAME>
```

Mode

Content Filter Profile Object

Description

Set forbidden uri list.

Options

<CONTENT_FILTER_URI_LIST_NAME> Content filter URI list object/group name.
Example: *White URI list*

Example

```
uri-list forbidden forbiddenUriListName
```

Syntax

```
no uri-list forbidden
```

Mode

Content Filter Profile Object

Description

Clear forbidden uri list.

Example

```
no uri-list forbidden
```

Syntax

```
uri-list search-order { allowed-first | forbidden-first }
```

Mode

Content Filter Profile Object

Description

Set uri list search order.

Options

allowed-first Search allowed URI list first.

forbidden-first Search forbidden URI list first.

Example

```
uri-list search-order allowed-first
```

Syntax

```
uri-list forbidden-operation <CONTENT_FILTER_FORBIDDEN_LIST_OPERATION_NAME>
```

Mode

Content Filter Profile Object

Description

Set operation of forbidden uri list.

Options

<CONTENT_FILTER_FORBIDDEN_LIST_OPERATION_NAME> Content filter operation for forbidden URI list.
Example: *block*

Example

```
uri-list operation-for-forbidden block
```

Syntax

```
category <CONTENT_FILTER_CATEGORY_ID_NAME> <CONTENT_FILTER_OPERATION_NAME>
```

Mode

Content Filter Profile Object

Description

Set operation of category.

Options

<CONTENT_FILTER_CATEGORY_ID_NAME> Content filter category number and name.
Example: *1. Violence/Hate/Racism*

<CONTENT_FILTER_OPERATION_NAME> Content filter operation.
Example: *block*

Example

```
category "1. Violence/Hate/Racism" block
```

Syntax

categories <CONTENT_FILTER_OPERATION_HAVING_DEFAULT_NAME>

Mode

Content Filter Profile Object

Description

Set operation for all categories.

Options

<CONTENT_FILTER_OPERATION_HAVING_DEFAULT_NAME> Content filter operation with additional \"default\".
Example: *default*

Example

categories default
categories block

Syntax

https-filtering

Mode

Content Filter Profile Object

Description

Enable CFS HTTPS filtering.

Example

https-filtering

Syntax

no https-filtering

Mode

Content Filter Profile Object

Description

Disable CFS HTTPS filtering.

Example

no https-filtering

Syntax

smart-filter

Mode

Content Filter Profile Object

Description

Enable smart filtering for embedded URI.

Example

smart-filter

Syntax

no smart-filter

Mode

Content Filter Profile Object

Description

Disable smart filtering for embedded URI.

Example

smart-filter

Syntax

safe-search

Mode

Content Filter Profile Object

Description

Enable safe search enforcement.

Example

safe-search

Syntax

no safe-search

Mode

Content Filter Profile Object

Description

Disable safe search enforcement.

Example

no safe-search

Syntax

threat-api

Mode

Content Filter Profile Object

Description

Enable threat api enforcement.

Example

threat-api

Syntax

no threat-api

Mode

Content Filter Profile Object

Description

Disable threat api enforcement.

Example

no threat-api

Syntax

google-force-safe-search

Mode

Content Filter Profile Object

Description

Enable Google force safe search.

Example

google-force-safe-search

Syntax

no google-force-safe-search

Mode

Content Filter Profile Object

Description

Disable Google force safe search.

Example

no google-force-safe-search

Syntax

youtube-restrict-mode

Mode

Content Filter Profile Object

Description

Enable YouTube restrict mode.

Example

youtube-restrict-mode

Syntax

no youtube-restrict-mode

Mode

Content Filter Profile Object

Description

Disable YouTube restrict mode.

Example

```
no youtube-restrict-mode
```

Syntax

```
bing-force-safe-search
```

Mode

Content Filter Profile Object

Description

Enable Bing force safe search.

Example

```
bing-force-safe-search
```

Syntax

```
no bing-force-safe-search
```

Mode

Content Filter Profile Object

Description

Disable Bing force safe search.

Example

```
no bing-force-safe-search
```

Syntax

```
consent required
```

Mode

Content Filter Profile Object

Description

Enable consent.

Example

```
consent required
```

Syntax

```
no consent required
```

Mode

Content Filter Profile Object

Description

Disable consent.

Example

```
no consent required
```

Syntax

```
consent user-idle-timeout <UINT32>
```

Mode

Content Filter Profile Object

Description

Set consent user idle timeout.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
consent user-idle-timeout 15
```

Syntax

```
consent optional page-url <WORD>
```

Mode

Content Filter Profile Object

Description

Set consent optional page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
consent optional page-url 1.1.1.1/consentOptional.html
```

Syntax

```
no consent optional page-url
```

Mode

Content Filter Profile Object

Description

Clear consent optional page URL.

Example

```
no consent optional page-url
```

Syntax

consent mandatory page-url <WORD>

Mode

Content Filter Profile Object

Description

Set consent mandatory page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

consent mandatory page-url 1.1.1.1/consentMandatory.html

Syntax

no consent mandatory page-url

Mode

Content Filter Profile Object

Description

Clear consent mandatory page URL.

Example

no consent mandatory page-url

Syntax

consent mandatory address { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group <ADDR_HNR_GROUP_MIXED> | name <ADDR_HNR_NAME_MIXED> }

Mode

Content Filter Profile Object

Description

Set consent mandatory filtering address.

Options

ipv6	IPv6 Address object.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

<i>any</i>	All address.
<i>group</i>	Address object group name.
<ADDR_HNR_GROUP_MIXED>	Host/network/range group address object name. Example: <i>Sales & Marketing Network Access Points</i>
<i>name</i>	Address object name.
<ADDR_HNR_NAME_MIXED>	Host/network/range address object name. Example: <i>Web Server</i>

Example

```
consent mandatory address host 192.168.168.168
consent mandatory address network 192.168.168.0 255.255.255.0
consent mandatory address range 192.168.168.1 192.168.168.10
consent mandatory address ipv6 host fec0:1::1
consent mandatory address ipv6 network fec0:1:: 64
consent mandatory address ipv6 range fec0:1::1 fec0:1::100
consent mandatory address any
consent mandatory address group "Consent Mandatory Address Group"
consent mandatory address name "Consent Mandatory Address Object"
```

Syntax

no consent mandatory address

Mode

Content Filter Profile Object

Description

Clear consent mandatory filtering address.

Example

no consent mandatory address

Syntax

custom-header insertion

Mode

Content Filter Profile Object

Description

Enable custom header insertion.

Example

custom-header insertion

Syntax

no custom-header insertion

Mode

Content Filter Profile Object

Description

Disable custom header insertion.

Example

no custom-header insertion

Syntax

```
custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter Profile Object

Description

Add new custom header entry into custom header list.

Options

<CONTENT_FILTER_CUSTOM_HEADER_DOMAIN>	Content filter custom header domain. Example: <code>\ "YouTube.com\"</code>
<CONTENT_FILTER_CUSTOM_HEADER_KEY>	Content filter custom header key. Example: <code>\ "YouTube-Restrict-Mode\"</code>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>	Content filter custom header value. Example: <code>\ "Strict\"</code>

Example

```
custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

```
no custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter Profile Object

Description

Delete custom header entry from custom header list.

Options

<CONTENT_FILTER_CUSTOM_HEADER_DOMAIN>	Content filter custom header domain. Example: <code>\ "YouTube.com\"</code>
<CONTENT_FILTER_CUSTOM_HEADER_KEY>	Content filter custom header key. Example: <code>\ "YouTube-Restrict-Mode\"</code>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>	Content filter custom header value. Example: <code>\ "Strict\"</code>

Example

```
no custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

```
no custom-header entries
```

Mode

Content Filter Profile Object

Description

Remove all custom header entries from custom header list.

Example

```
no custom-header entries
```

Syntax

uuid <UUID>

Mode

Content Filter URI List Object

Description

Select URI list object by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid "00000000-0000-0001-0f00-c0eae49ce84c"

Syntax

no uuid

Mode

Content Filter URI List Object

Description

Delete URI list object by UUID.

Example

uuid "00000000-0000-0001-0f00-c0eae49ce84c"

Syntax

uuid <UUID>

Mode

Content Filter URI List Group

Description

Select URI list group Uuid.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid "00000000-0000-0001-0f00-c0eae49ce84c"

Syntax

no uuid

Mode

Description

Delete URI list group by UUID.

Example

```
uuid "00000000-0000-0001-1000-c0eae49ce84c"
```

Syntax

```
uuid <UUID>
```

Mode

Content Filter Action Object

Description

Select CFS action object by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid "9939f8b6-a6bc-d435-0d00-c0eae49ce84c"
```

Syntax

```
no uuid
```

Mode

Content Filter Action Object

Description

Delete Action object by UUID.

Example

```
uuid "9939f8b6-a6bc-d435-0d00-c0eae49ce84c"
```

Syntax

```
uuid <UUID>
```

Mode

Content Filter Profile Object

Description

Select CFS profile object by UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid "731af6e4-bf29-47b7-0e00-c0eae49ce84c"
```

Syntax

```
no uuid
```

Mode

Content Filter Profile Object

Description

Delete CFS profile object by UUID.

Example

```
uuid "731af6e4-bf29-47b7-0e00-c0eae49ce84c"
```

Syntax

```
server <WORD>
```

Mode

Websense enterprise

Description

Set Websense server address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
server 192.168.168.100
```

Syntax

```
no server
```

Mode

Websense enterprise

Description

Clear Websense server address.

Example

```
no server
```

Syntax

```
port <IPV4_PORT>
```

Mode

Websense enterprise

Description

Set Websense server port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

port 15868

Syntax

user-name <WORD>

Mode

Websense enterprise

Description

Set user name of Websense.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name userName

Syntax

no user-name

Mode

Websense enterprise

Description

Clear user name of Websense.

Example

no user-name

Syntax

max-url-caches <UINT32>

Mode

Websense enterprise

Description

Set maximum URL cache entries that can be added.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

max-url-caches 5120

Syntax

https-content-filtering

Mode

Websense enterprise

Description

Enable https content filtering.

Example

https-content-filtering

Syntax

no https-content-filtering

Mode

Websense enterprise

Description

Disable https content filtering.

Example

no https-content-filtering

Syntax

probe monitoring

Mode

Websense enterprise

Description

Enable Websense probe monitoring.

Example

probe monitoring

Syntax

no probe monitoring

Mode

Websense enterprise

Description

Disable Websense probe monitoring.

Example

no probe monitoring

Syntax

probe interval <UINT16>

Mode

Websense enterprise

Description

Set check server interval in seconds of Websense probe monitoring.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
probe interval 10
```

Syntax

```
probe deactivate-after <UINT8>
```

Mode

Websense enterprise

Description

Set deactivation condition of Websense.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
probe deactivate-after 3
```

Syntax

```
probe reactivate-after <UINT8>
```

Mode

Websense enterprise

Description

Set reactivation condition of Websense.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
probe reactivate-after 2
```

Syntax

```
block-if-server-unavailable
```

Mode

Websense enterprise

Description

Enable block if Websense server is unavailable.

Example

block-if-server-unavailable

Syntax

no block-if-server-unavailable

Mode

Websense enterprise

Description

Disable block if Websense server is unavailable.

Example

no block-if-server-unavailable

Syntax

server-timeout <UINT16>

Mode

Websense enterprise

Description

Set Websense server timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

server-timeout 5

Syntax

block activex

Mode

Websense enterprise

Description

Enable block ActiveX feature.

Example

block activex

Syntax

no block activex

Mode

Websense enterprise

Description

Disable block ActiveX feature.

Example

```
no block activex
```

Syntax

```
block java
```

Mode

Websense enterprise

Description

Enable block Java feature.

Example

```
block java
```

Syntax

```
no block java
```

Mode

Websense enterprise

Description

Disable block Java feature.

Example

```
no block java
```

Syntax

```
block flash
```

Mode

Websense enterprise

Description

Enable block Flash feature.

Example

```
block flash
```

Syntax

```
no block flash
```

Mode

Websense enterprise

Description

Disable block Flash feature.

Example

```
no block flash
```

Syntax

```
block cookies
```

Mode

Websense enterprise

Description

Enable block cookies feature.

Example

```
block cookies
```

Syntax

```
no block cookies
```

Mode

Websense enterprise

Description

Disable block cookies feature.

Example

```
no block cookies
```

Syntax

```
block http-proxy-access
```

Mode

Websense enterprise

Description

Enable block access to HTTP proxy feature.

Example

```
block http-proxy-access
```

Syntax

```
no block http-proxy-access
```

Mode

Websense enterprise

Description

Disable block Access to HTTP Proxy feature.

Example

```
no block http-proxy-access
```

Syntax

exclude web-features-domains <CONTENT_FILTER_URI_LIST_NAME>

Mode

Websense enterprise

Description

Set excluded domains of block web features.

Options

<CONTENT_FILTER_URI_LIST_NAME> Content filter URI list object/group name.
Example: *White URI list*

Example

exclude web-features-domains uriListName

Syntax

no exclude web-features-domains

Mode

Websense enterprise

Description

Clear excluded domains of block web features.

Example

no exclude web-features-domains

Syntax

exclude administrator

Mode

Websense enterprise

Description

Enable exclude administrator.

Example

exclude administrator

Syntax

no exclude administrator

Mode

Websense enterprise

Description

Disable exclude administrator.

Example

no exclude administrator

Syntax

exclude address { { [ipv6] { fqdn <ADDR_FQDN> | host <ADDR_HOST> | mac <ADDR_MAC> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Websense enterprise

Description

Exclude address.

Options

ipv6	IPv6 Address object.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Address object MAC Address. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Address object group name. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

exclude address host 192.168.168.168
exclude address network 192.168.168.0 255.255.255.0
exclude address range 192.168.168.1 192.168.168.10
exclude address mac D067E534E99C
exclude address fqdn example.com
exclude address ipv6 host fec0:1::1
exclude address ipv6 network fec0:1:: 64
exclude address ipv6 range fec0:1::1 fec0:1::100
exclude address group "Corp Websense Exclusion Group"
exclude address name "Corp Websense Exclusion Object"

Syntax

no exclude address

Mode

Websense enterprise

Description

Clear excluded address.

Example

```
no exclude address
```

Syntax

```
blocking-page { custom <WORD> | default }
```

Mode

Websense enterprise

Description

Set Websense blocking page.

Options

custom Use custom defined page.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

default Use default page.

Example

```
blocking-page custom "<html> ... </html>"  
blocking-page default
```

Syntax

```
endpoint-security
```

Mode

Config

Description

Enter Endpoint Security configuration mode.

Example

```
endpoint-security
```

Syntax

```
enable
```

Mode

Endpoint Security

Description

Enable Endpoint Security.

Example

```
enable
```

Syntax

no enable

Mode

Endpoint Security

Description

Disable Endpoint Security.

Example

no enable

Syntax

alert-message enable

Mode

Endpoint Security

Description

Enable Alert Message to Endpoint Devices via Capture Client Endpoint Security.

Example

alert-message enable

Syntax

no alert-message enable

Mode

Endpoint Security

Description

Disable Alert Message to Endpoint Devices via Capture Client Endpoint Security.

Example

no alert-message enable

Syntax

log cfs

Mode

Endpoint Security

Description

Enable Logging CFS Message to Endpoint Devices via Capture Client Endpoint Security.

Example

log cfs

Syntax

no log cfs

Mode

Endpoint Security

Description

Disable Logging CFS Message to Endpoint Devices via Capture Client Endpoint Security.

Example

no log cfs

Syntax

log ips

Mode

Endpoint Security

Description

Enable Logging IPS Message to Endpoint Devices via Capture Client Endpoint Security.

Example

log ips

Syntax

no log ips

Mode

Endpoint Security

Description

Disable Logging IPS Message to Endpoint Devices via Capture Client Endpoint Security.

Example

no log ips

Syntax

log appctrl

Mode

Endpoint Security

Description

Enable Logging APP Control Message to Endpoint Devices via Capture Client Endpoint Security.

Example

log appctrl

Syntax

no log appctrl

Mode

Endpoint Security

Description

Disable Logging APP Control Message to Endpoint Devices via Capture Client Endpoint Security.

Example

```
no log control
```

Syntax

```
log botnet-geoip
```

Mode

Endpoint Security

Description

Enable Logging Botnet/Geo-IP Message to Endpoint Devices via Capture Client Endpoint Security.

Example

```
log botnet-geoip
```

Syntax

```
no log botnet-geoip
```

Mode

Endpoint Security

Description

Disable Logging Botnet/Geo-IP Message to Endpoint Devices via Capture Client Endpoint Security.

Example

```
no log botnet-geoip
```

Syntax

```
log gav-gas-atp
```

Mode

Endpoint Security

Description

Enable Logging GAV/GAS/ATP Message to Endpoint Devices via Capture Client Endpoint Security.

Example

```
log gav-gas-atp
```

Syntax

```
no log gav-gas-atp
```

Mode

Endpoint Security

Description

Disable Logging GAV/GAS/ATP Message to Endpoint Devices via Capture Client Endpoint Security.

Example

```
no log gav-gas-atp
```

Syntax

```
user-sso enable
```

Mode

Endpoint Security

Description

Enable endpoint device user authentication via Capture Client Endpoint Security.

Example

```
user-sso enable
```

Syntax

```
no user-sso enable
```

Mode

Endpoint Security

Description

Disable endpoint device user authentication via Capture Client Endpoint Security.

Example

```
no user-sso enable
```

Syntax

```
no profiles
```

Mode

Endpoint Security

Description

Delete all Endpoint Enforcement Profiles.

Example

```
no profiles
```

Syntax

```
no profile <ENDPOINT_SECURITY_PROFILE_NAME>
```

Mode

Endpoint Security

Description

Delete Endpoint Enforcement Profile.

Options

<ENDPOINT_SECURITY_PROFILE_NAME> Endpoint security profile object name.
Example: *Market profile*

Example

no profile profileName

Syntax

profile <ENDPOINT_SECURITY_PROFILE_NAME>

Mode

Endpoint Security

Description

Add/Edit Endpoint Enforcement Profile and enter configuration mode.

Options

<ENDPOINT_SECURITY_PROFILE_NAME> Endpoint security profile object name.
Example: *Market profile*

Example

profile profileName

Syntax

name <ENDPOINT_SECURITY_PROFILE_NAME>

Mode

Endpoint Enforcement Profile

Description

Set profile object name.

Options

<ENDPOINT_SECURITY_PROFILE_NAME> Endpoint security profile object name.
Example: *Market profile*

Example

name profileName

Syntax

grace-period <UINT32>

Mode

Endpoint Enforcement Profile

Description

Set grace period (measured in days) for Endpoint Security services in profile.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

grace-period 5

Syntax

no grace-period

Mode

Endpoint Enforcement Profile

Description

Set grace period (measured in days) as ZERO for Endpoint Security services in profile.

Example

no grace-period

Syntax

bypass-guest-ce

Mode

Endpoint Enforcement Profile

Description

Enable Bypass Guest Endpoint Security Service.

Example

bypass-guest-ce

Syntax

no bypass-guest-ce

Mode

Endpoint Enforcement Profile

Description

Disable Bypass Guest Endpoint Security Service.

Example

no bypass-guest-ce

Syntax

service-capture-client

Mode

Endpoint Enforcement Profile

Description

Enable capture client endpoint security service.

Example

service-capture-client

Syntax

```
no service-capture-client
```

Mode

Endpoint Enforcement Profile

Description

Disable capture client endpoint security service.

Example

```
no service-capture-client
```

Syntax

```
no policies
```

Mode

Endpoint Security

Description

Delete all Endpoint Security policies.

Example

```
no policies
```

Syntax

```
no policy <ENDPOINT_SECURITY_POLICY_NAME>
```

Mode

Endpoint Security

Description

Delete Endpoint Enforcement Policy.

Options

<ENDPOINT_SECURITY_POLICY_NAME> Endpoint security policy name.
Example: *Market policy*

Example

```
no policy "policyName"
```

Syntax

```
policy <ENDPOINT_SECURITY_POLICY_NAME>
```

Mode

Endpoint Security

Description

Add/Edit Endpoint Enforcement Policy and enter configuration mode.

Options

<ENDPOINT_SECURITY_POLICY_NAME> Endpoint security policy name.
Example: *Market policy*

Example

```
policy "Endpoint Enforcement default policy"
```

Syntax

```
name <ENDPOINT_SECURITY_POLICY_NAME>
```

Mode

Endpoint Enforcement Policy

Description

Set policy name.

Options

- <ENDPOINT_SECURITY_POLICY_NAME> Endpoint security policy name.
Example: *Market policy*

Example

```
name "Endpoint Enforcement default policy"
```

Syntax

```
source zone <ENDPOINT_SECURITY_POLICY_ZONE>
```

Mode

Endpoint Enforcement Policy

Description

Set source zone.

Options

- <ENDPOINT_SECURITY_POLICY_ZONE> Endpoint security policy zone.
Example: *LAN*

Example

```
source zone LAN
```

Syntax

```
source address included { { [ ipv6 ] { host <ENDPOINT_SECURITY_POLICY_ADDR_HOST> | network  
<ENDPOINT_SECURITY_POLICY_ADDR_NETWORK> <ENDPOINT_SECURITY_POLICY_ADDR_MASK> | range <ENDPOINT_SECURITY_POLICY_ADDR_BEGIN>  
<ENDPOINT_SECURITY_POLICY_ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name  
<ADDR_NAME_MIXED> }
```

Mode

Endpoint Enforcement Policy

Description

Set included source address.

Options

- ipv6* IPv6 Address object.
- host* Address object host.
- <ENDPOINT_SECURITY_POLICY_ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network	Address object network.
<ENDPOINT_SECURITY_POLICY_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ENDPOINT_SECURITY_POLICY_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Specify IP range.
<ENDPOINT_SECURITY_POLICY_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ENDPOINT_SECURITY_POLICY_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group object name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC Address.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
source address included host 192.168.168.168
source address included network 192.168.168.0 255.255.255.0
source address included range 192.168.168.1 192.168.168.10
source address included mac D067E534E99C
source address included fqdn example.com
source address included ipv6 host fec0:1::1
source address included ipv6 network fec0:1:: 64
source address included ipv6 range fec0:1::1 fec0:1::100
source address included any
source address included group "Endpoint Enforcement Policy Source Address Group"
source address included name "Endpoint Enforcement Policy Source Address Object"
```

Syntax

```
source address excluded { { [ ipv6 ] { host <ENDPOINT_SECURITY_POLICY_ADDR_HOST> | network
<ENDPOINT_SECURITY_POLICY_ADDR_NETWORK> <ENDPOINT_SECURITY_POLICY_ADDR_MASK> | range <ENDPOINT_SECURITY_POLICY_ADDR_BEGIN>
<ENDPOINT_SECURITY_POLICY_ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name
<ADDR_NAME_MIXED> | none }
```

Mode

Endpoint Enforcement Policy

Description

Set excluded source address.

Options

ipv6	IPv6 Address object.
host	Address object host.
<ENDPOINT_SECURITY_POLICY_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

network	Address object network.
<ENDPOINT_SECURITY_POLICY_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ENDPOINT_SECURITY_POLICY_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Specify IP range.
<ENDPOINT_SECURITY_POLICY_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ENDPOINT_SECURITY_POLICY_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group object name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC Address.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
none	None address.

Example

```
source address excluded host 192.168.168.168
source address excluded network 192.168.168.0 255.255.255.0
source address excluded range 192.168.168.1 192.168.168.10
source address excluded mac D067E534E99C
source address excluded fqdn example.com
source address excluded ipv6 host fec0:1::1
source address excluded ipv6 network fec0:1:: 64
source address excluded ipv6 range fec0:1::1 fec0:1::100
source address excluded none
source address excluded group "CFS Policy Source Address Group"
source address excluded name "CFS Policy Source Address Object"
```

Syntax

```
profile <ENDPOINT_SECURITY_PROFILE_NAME>
```

Mode

Endpoint Enforcement Policy

Description

Set profile.

Options

<ENDPOINT_SECURITY_PROFILE_NAME> Endpoint security profile object name.
Example: *Market profile*

Example

```
profile "Endpoint Enforcement Default profile"
```

Syntax

```
enable
```

Mode

Endpoint Enforcement Policy

Description

Enable the policy.

Example

enable

Syntax

no enable

Mode

Endpoint Enforcement Policy

Description

Disable the policy.

Example

no enable

Syntax

priority <UINT32>

Mode

Endpoint Enforcement Policy

Description

Set priority.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

priority 3

Syntax

no priority

Mode

Endpoint Enforcement Policy

Description

Clear priority.

Example

no priority

Syntax

anti-spam

Mode

Config

Description

Enter anti-spam configuration mode.

Example

anti-spam

Syntax

start anti-spam-capture

Mode

Anti-Spam
Top Level
Config

Description

Start e-mail stream packet capture.

Example

start anti-spam-capture

Syntax

stop anti-spam-capture

Mode

Anti-Spam
Top Level
Config

Description

Stop e-mail stream packet capture.

Example

stop anti-spam-capture

Syntax

clear anti-spam-capture

Mode

Anti-Spam
Top Level
Config

Description

Clear the e-mail stream packet capture buffer.

Example

clear anti-spam-capture

Syntax

```
export capture { ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Anti-Spam

Description

Download e-mail stream capture data.

Options

ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Export using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
export capture ftp ftp://user:password@servername/packet-hd.html
export capture scp user@server:/home/user/packet-hd.html
export capture scp user@server:/home/user/
```

Syntax

```
grid-ip-check <IPV4_HOST>
```

Mode

Top Level
Config
Anti-Spam

Description

Do the IP reputation check with the SonicWall GRID network with the given ip address.

Options

<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
grid-ip-check 10.10.10.10
```

Syntax

```
enable
```

Mode

Anti-Spam

Description

Enable anti-spam service.

Example

```
enable
```

Syntax

```
destination-mail-server public <IPV4_HOST> private <IPV4_HOST> zone <ANTI_SPAM_DMS_ZONE> port <IPV4_PORT>
```

Mode

Anti-Spam

Description

Set the destination mail server configuration.

Options

<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
private	Set the destination mail server public IP.
<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
zone	Set the destination mail server zone assignment.
<ANTI_SPAM_DMS_ZONE>	Zone object name. Example: <i>DMZ</i>
port	Set the destination mail server inbound e-mail port.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
destination-mail-server public 192.168.168.110 private 192.168.1.2 zone LAN port 25
```

Syntax

```
no enable
```

Mode

Anti-Spam

Description

Disable anti-spam service.

Example

```
no enable
```

Syntax

```
action likely-spam { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the likely spam category.

Options

delete	Permanently delete.
filtering-off	Filtering off.
store	Store in junk box.
tag	Tag the email.

Example

action likely-spam filtering-off

Syntax

action definite-spam { delete | filtering-off | store | tag }

Mode

Anti-Spam

Description

Set the action for the definite spam category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

action definite-spam tag

Syntax

action likely-phishing { delete | filtering-off | store | tag }

Mode

Anti-Spam

Description

Set the action for the likely phishing category.

Options

delete Permanently delete.

filtering-off Filtering off.

store Store in junk box.

tag Tag the email.

Example

action likely-phishing tag

Syntax

action definite-phishing { delete | filtering-off | store | tag }

Mode

Anti-Spam

Description

Set the action for the definite phishing category.

Options

<i>delete</i>	Permanently delete.
<i>filtering-off</i>	Filtering off.
<i>store</i>	Store in junk box.
<i>tag</i>	Tag the email.

Example

```
action definite-phishing delete
```

Syntax

```
action likely-virus { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the likely spam category.

Options

<i>delete</i>	Permanently delete.
<i>filtering-off</i>	Filtering off.
<i>store</i>	Store in junk box.
<i>tag</i>	Tag the email.

Example

```
action likely-virus tag
```

Syntax

```
action definite-virus { delete | filtering-off | store | tag }
```

Mode

Anti-Spam

Description

Set the action for the definite virus category.

Options

<i>delete</i>	Permanently delete.
<i>filtering-off</i>	Filtering off.
<i>store</i>	Store in junk box.
<i>tag</i>	Tag the email.

Example

```
action definite-virus delete
```

Syntax

```
allow-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range <ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Add address object to the allow client list.

Options

<i>fqdn</i>	Address object full qualified domain name (FQDN).
<ANTI_SPAM_ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	Address object host.
<ANTI_SPAM_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ANTI_SPAM_ADDR_NAME>	Address object name. Example: <i>Web Server</i>
<i>range</i>	Address object range.
<ANTI_SPAM_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ANTI_SPAM_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
allow-list host 168.226.49.15
allow-list name "X3 IP"
allow-list range 192.168.1.100 192.168.1.150
allow-list fqdn "www.sonicwall.com"
```

Syntax

```
no allow-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range <ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Remove address object from the allow client list.

Options

<i>fqdn</i>	Address object full qualified domain name (FQDN).
<ANTI_SPAM_ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	Address object host.
<ANTI_SPAM_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ANTI_SPAM_ADDR_NAME>	Address object name.

Example: *Web Server*

<i>range</i>	Address object range.
<ANTI_SPAM_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ANTI_SPAM_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
no allow-list host 168.226.49.15
no allow-list name "X3 IP"
no allow-list range 192.168.1.100 192.168.1.150
no allow-list fqdn "www.sonicwall.com"
```

Syntax

```
reject-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range
<ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Add address object to the reject client list.

Options

<i>fqdn</i>	Address object full qualified domain name (FQDN).
<ANTI_SPAM_ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	Address object host.
<ANTI_SPAM_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ANTI_SPAM_ADDR_NAME>	Address object name. Example: <i>Web Server</i>
<i>range</i>	Address object range.
<ANTI_SPAM_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ANTI_SPAM_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
reject-list host 168.226.49.15
reject-list name "X3 IP"
reject-list range 192.168.1.100 192.168.1.150
reject-list fqdn "www.sonicwall.com"
```

Syntax

```
no reject-list { fqdn <ANTI_SPAM_ADDR_FQDN> | host <ANTI_SPAM_ADDR_HOST> | name <ANTI_SPAM_ADDR_NAME> | range
<ANTI_SPAM_ADDR_BEGIN> <ANTI_SPAM_ADDR_END> }
```

Mode

Anti-Spam

Description

Remove address object from the reject client list.

Options

<i>fqdn</i>	Address object full qualified domain name (FQDN).
<ANTI_SPAM_ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	Address object host.
<ANTI_SPAM_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<ANTI_SPAM_ADDR_NAME>	Address object name. Example: <i>Web Server</i>
<i>range</i>	Address object range.
<ANTI_SPAM_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ANTI_SPAM_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
no reject-list host 168.226.49.15
no reject-list name "X3 IP"
no reject-list range 192.168.1.100 192.168.1.150
no reject-list fqdn "www.sonicwall.com"
```

Syntax

```
service-down { allow | reject }
```

Mode

Anti-Spam

Description

Set action of delivery of unprocessed mail when SonicWall anti-spam service is unavailable.

Options

<i>allow</i>	Allow.
<i>reject</i>	Reject.

Example

```
service-down reject
service-down allow
```

Syntax

```
junk-box down { delete | tag-deliver }
```

Mode

Anti-Spam

Description

Set action for e-mails when junk box is unavailable.

Options

- delete*** Delete.
- tag-deliver*** Tag and deliver.

Example

```
junk-box down tag-deliver
junk-box down delete
```

Syntax

```
junk-box secure-http
```

Mode

Anti-Spam

Description

Enable use secure HTTP for junk box messaging.

Example

```
junk-box secure-http
```

Syntax

```
no junk-box secure-http
```

Mode

Anti-Spam

Description

Disable use secure HTTP for junk box messaging.

Example

```
no junk-box secure-http
```

Syntax

```
junk-box port <IPV4_PORT>
```

Mode

Anti-Spam

Description

Set the junk box messaging port.

Options

- <IPV4_PORT>*** Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
junk-box port 80
```

Syntax

```
no junk-box port
```


Mode

Anti-Spam

Description

Clear the junk box messaging port.

Example

```
no junk-box port
```

Syntax

```
probe interval <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe interval in minutes.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
probe interval 5
```

Syntax

```
probe timeout <UINT16>
```

Mode

Anti-Spam

Description

Set the monitoring service probe timeout in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
probe timeout 30
```

Syntax

```
success-threshold <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe success count threshold.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
success-threshold 1
```

Syntax

```
failure-threshold <UINT8>
```

Mode

Anti-Spam

Description

Set the monitoring service probe failure count threshold.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
failure-threshold 3
```

Syntax

```
mail-server { port <IPV4_PORT> | private <IPV4_HOST> | public <IPV4_HOST> }
```

Mode

Anti-Spam

Description

Set the destination mail server public IP address, private IP address and inbound e-mail port.

Options

port Set the destination mail server inbound e-mail port.
<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

private Set the destination mail server private IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

public Set the destination mail server public IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
mail-server private 192.168.168.10
mail-server public 192.168.168.110
mail-server port 25
```

Syntax

```
no mail-server { port | private | public }
```

Mode

Anti-Spam

Description

Clear the destination mail server public or private IP address or inbound e-mail port.

Options

port Clear the destination mail server inbound e-mail port.

private Clear the destination mail server private IP address.

public Clear the destination mail server public IP address.

Example

```
no mail-server ip private
no mail-server ip public
no mail-server port
```

Syntax

```
junk-store-username <WORD>
```

Mode

Anti-Spam

Description

Set junk store username.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
junk-store-username admin
```

Syntax

```
junk-store-password <ENC_PASSWORD>
```

Mode

Anti-Spam

Description

Set junk store password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
junk-store-password *****
```

Syntax

```
destination-mail-address-as-junk-store
```

Mode

Anti-Spam

Description

Enable use destination mail server private address as junk store IP address.

Example

```
destination-mail-address-as-junk-store
```

Syntax

```
no destination-mail-address-as-junk-store
```

Mode

Anti-Spam

Description

Disable use destination mail server private address as junk store IP address.

Example

```
no destination-mail-address-as-junk-store
```

Syntax

```
junk-store-ip <IPV4_HOST>
```

Mode

Anti-Spam

Description

Set junk store ip address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
junk-store-ip 192.168.168.168
```

Syntax

```
no junk-store-ip
```

Mode

Anti-Spam

Description

Clear junk store ip address.

Example

```
no junk-store-ip
```

Syntax

```
system-detection
```

Mode

Anti-Spam

Description

Enable e-mail system detection.

Example

```
system-detection
```

Syntax

```
no system-detection
```

Mode

Anti-Spam

Description

Disable e-mail system detection.

Example

```
no system-detection
```

Syntax

```
intrusion-prevention
```

Mode

Config

Description

Enter intrusion prevention configuration mode.

Example

```
intrusion-prevention
```

Syntax

```
update-signatures
```

Mode

IPS

Description

Update signature database.

Example

```
update-signatures
```

Syntax

```
enable
```

Mode

IPS

Description

Enable intrusion prevention.

Example

```
enable
```

Syntax

```
no enable
```

Mode

IPS

Description

Disable intrusion prevention.

Example

```
no enable
```

Syntax

```
signature-group high-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group high priority detection and log redundancy.

Options

<i>detect-all</i>	Detect all.
<i>log-redundancy</i>	Set log redundancy in seconds.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>prevent-all</i>	Prevent all.

Example

```
signature-group high-priority prevent-all  
signature-group high-priority log-redundancy 60
```

Syntax

```
signature-group medium-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group medium priority detection and log redundancy.

Options

<i>detect-all</i>	Detect all.
<i>log-redundancy</i>	Set log redundancy in seconds.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>

prevent-all Prevent all.

Example

```
signature-group medium-priority prevent-all
signature-group medium-priority log-redundancy 60
```

Syntax

```
signature-group low-priority { detect-all | log-redundancy <UINT32> | prevent-all }
```

Mode

IPS

Description

Enable signature group low priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

prevent-all Prevent all.

Example

```
signature-group low-priority prevent-all
signature-group low-priority log-redundancy 60
```

Syntax

```
no signature-group high-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group high priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Clear log redundancy.

prevent-all Prevent all.

Example

```
no signature-group high-priority prevent-all
no signature-group high-priority log-redundancy
```

Syntax

```
no signature-group medium-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group medium priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Clear log redundancy.

prevent-all Prevent all.

Example

```
no signature-group medium-priority prevent-all
no signature-group medium-priority log-redundancy
```

Syntax

```
no signature-group low-priority { detect-all | log-redundancy | prevent-all }
```

Mode

IPS

Description

Disable signature group low priority detection and log redundancy.

Options

detect-all Detect all.

log-redundancy Clear log redundancy.

prevent-all Prevent all.

Example

```
no signature-group low-priority prevent-all
no signature-group low-priority log-redundancy
```

Syntax

```
reset
```

Mode

IPS

Description

Reset intrusion prevention settings to default.

Example

```
reset
```

Syntax

```
category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } [ policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } ]
```

Mode

Description

Enter configuration mode for the specified IPS category.

Options

<i>id</i>	IPS category ID.
<i><IPS_CATEGORY_ID></i>	Category ID. Example: <i>1234</i>
<i>name</i>	IPS category name.
<i><IPS_CATEGORY_NAME></i>	Category name. Example: <i>ACTIVEX</i>
<i>policy</i>	Configure the IPS policy and enter its configure mode.
<i>id</i>	IPS policy ID.
<i><IPS_POLICY_ID></i>	Policy ID. Example: <i>1234</i>
<i>name</i>	IPS policy name.
<i><IPS_POLICY_NAME></i>	Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i>

Example

```
category name "BACKDOOR"
category id 2 policy id 6483
category id 61 policy name "ActivePDF WebGrabber ActiveX Instantiation"
```

Syntax

```
exclusion { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | address {
{ object | range } } | entry <IPS_EXCLUSION_BEGIN_IPV4_HOST> <IPS_EXCLUSION_END_IPV4_HOST> | group <ADDR_GROUP_NAME_MIXED> |
list | name <ADDR_NAME_MIXED> }
```

Mode

IPS

Description

Configure IPS exclusion list.

Options

<i>ipv6</i>	Excluded IPv6 addresses.
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i>	Address object network.
<i><ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Address object range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>address</i>	Set exclusion list method.

<i>object</i>	Set exclusion list with address object.
<i>range</i>	Set exclusion list with address range.
<i>entry</i>	IPS exclusion list entry.
<i><IPS_EXCLUSION_BEGIN_IPV4_HOST></i>	IPS Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
<i><IPS_EXCLUSION_END_IPV4_HOST></i>	IPS Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
<i>group</i>	Address object group
<i><ADDR_GROUP_NAME_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>list</i>	Enable IPS exclusion list.
<i>name</i>	Address object name
<i><ADDR_NAME_MIXED></i>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion list
exclusion name "WLAN Subnets"
exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
from <IPS_EXCLUSION_BEGIN_IPV4_HOST>
```

Mode

IPS Exclusion Entry

Description

Set IPS exclusion list entry start ip.

Options

```
<IPS_EXCLUSION_BEGIN_IPV4_HOST> IPS Exclusion List entry begin IPv4 in the form: D.D.D.D.
Example: 192.168.168.168
```

Example

```
from 10.10.10.1
```

Syntax

```
to <IPS_EXCLUSION_END_IPV4_HOST>
```

Mode

IPS Exclusion Entry

Description

Set IPS exclusion list entry end ip.

Options

```
<IPS_EXCLUSION_END_IPV4_HOST> IPS Exclusion List entry end IPv4 in the form: D.D.D.D.
Example: 192.168.168.168
```

Example

```
to 10.10.10.1
```

Syntax

```
no exclusion { entries | entry <IPS_EXCLUSION_BEGIN_IPV4_HOST> <IPS_EXCLUSION_END_IPV4_HOST> | list }
```

Mode

IPS

Description

Disable IPS exclusion list.

Options

entries	Delete all IPS exclusion list entries.
entry	Delete one IPS exclusion list entry.
<IPS_EXCLUSION_BEGIN_IPV4_HOST>	IPS Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: 192.168.168.168
<IPS_EXCLUSION_END_IPV4_HOST>	IPS Exclusion List entry end IPv4 in the form: D.D.D.D. Example: 192.168.168.168
list	Disable IPS exclusion list.

Example

```
no exclusion list
no exclusion entries
no exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
name <WORD>
```

Mode

IPS Category
IPS Policy

Description

Category name or policy name.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: abc

Example

```
name ACTIVEX
```

Syntax

```
id <UINT32>
```

Mode

IPS Category
IPS Policy

Description

Category ID or policy ID.

Options

<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123

Example

Syntax

```
prevention [ enable | global ]
```

Mode

IPS Category

Description

Set prevention for IPS category.

Options

enable Enable IPS category prevention.

global Use global setting.

Example

```
prevention global
```

Syntax

```
no prevention
```

Mode

IPS Category

Description

Disable prevention for IPS category.

Example

```
no prevention
```

Syntax

```
detection [ enable | global ]
```

Mode

IPS Category

Description

Set detection for IPS category.

Options

enable Enable IPS category detection.

global Use global setting.

Example

```
detection global
```

Syntax

no detection

Mode

IPS Category

Description

Disable detection for IPS category.

Example

no detection

Syntax

included users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

IPS Category

Description

Set included users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>all</i>	All.
<i>group</i> <i><LOCAL_USER_GROUP_NAME></i>	Specify local user group. Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.
<i>name</i> <i><LOCAL_USER_NAME></i>	Specify local user. Local user object name. Example: <i>user1</i>

Example

included users all

Syntax

excluded users { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

IPS Category

Description

Set excluded users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>group</i> <i><LOCAL_USER_GROUP_NAME></i>	Specify local user group. Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.

<i>name</i>	Specify local user.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

excluded users guests

Syntax

```
included ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all |
group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Category

Description

Set included IP address range.

Options

<i>ipv6</i>	Included IPv6 addresses.
<i>host</i> <i><ADDR_HOST></i>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i> <i><ADDR_NETWORK></i>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <i><ADDR_BEGIN></i>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>all</i>	All.
<i>group</i> <i><ADDR_GROUP_NAME_MIXED></i>	Address object group. Group address object name. Example: <i>Sales Group</i>
<i>name</i> <i><ADDR_NAME_MIXED></i>	Specify name of range address object. Address object name. Example: <i>Web Server</i>

Example

included ip range 10.10.10.1 10.10.10.10

Syntax

```
excluded ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group
<ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Category

Description

Set excluded IP address range.

Options

ipv6	Excluded IPv6 addresses.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Address object group. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Specify name of range address object. Address object name. Example: <i>Web Server</i>

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

IPS Category

Description

Don't excluded any users/groups or IP addresses.

Options

ip	Don't excluded any IP addresses.
users	Don't excluded any users/groups.

Example

```
no excluded users  
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

IPS Category

Description

Set IPS category schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule always-on

Syntax

log-redundancy { filter <UINT16> | global }

Mode

IPS Category

Description

Set IPS category log redundancy filter.

Options

<i>filter</i>	Set log redundancy filter in seconds.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>global</i>	Use global setting.

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

IPS Category

Description

Clear IPS category log redundancy filter.

Options

<i>filter</i>	Clear log redundancy filter in seconds.

Example

no log-redundancy filter

Syntax

category <WORD>

Mode

IPS Policy

Description

IPS policy's category name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

category *ACTIVEX*

Syntax

prevention [*category* | *enable*]

Mode

IPS Policy

Description

Set prevention for IPS policy.

Options

category Use category setting.

enable Enable IPS policy prevention.

Example

prevention *category*

Syntax

no prevention

Mode

IPS Policy

Description

Disable prevention for IPS policy.

Example

no prevention

Syntax

detection [*category* | *enable*]

Mode

IPS Policy

Description

Set detection for IPS policy.

Options

- category** Use category setting.
- enable** Enable IPS policy detection.

Example

detection category

Syntax

no detection

Mode

IPS Policy

Description

Disable detection for IPS policy.

Example

no detection

Syntax

included users { administrator | all | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

IPS Policy

Description

Set included users/groups.

Options

- administrator** Built-in administrator.
- all** All.
- category** Use category setting.
- group** Specify local user group.
<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*
- guests** Guests.
- name** Specify local user.
<LOCAL_USER_NAME> Local user object name.
Example: *user1*

Example

included users all

Syntax

excluded users { administrator | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

IPS Policy

Description

Set excluded users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>category</i>	Use category setting.
<i>group</i>	Specify local user group.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.
<i>name</i>	Specify local user.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

excluded users guests

Syntax

included ip { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | category | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

IPS Policy

Description

Set included IP address range.

Options

<i>ipv6</i>	Included IPv6 addresses.
<i>host</i> <i><ADDR_HOST></i>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i>network</i> <i><ADDR_NETWORK></i>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <i><ADDR_BEGIN></i>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>
<i>all</i>	All.

category	Use category setting.
group	Address object group.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } |
category | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

IPS Policy

Description

Set excluded IP address range.

Options

ipv6	Excluded IPv6 addresses.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
category	Use category setting.
group	Address object group.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

IPS Policy

Description

Don't excluded any users/groups or IP addresses.

Options

ip	Don't excluded any IP addresses.
users	Don't excluded any users/groups.

Example

no excluded users
no excluded ip

Syntax

schedule { always-on | category | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

IPS Policy

Description

Set IPS policy schedule.

Options

always-on	Always on.
category	Use category setting.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule always-on

Syntax

log-redundancy { category | filter <UINT16> }

Mode

IPS Policy

Description

Set IPS policy log redundancy filter.

Options

category Use category setting.

filter Set log redundancy filter in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

IPS Policy

Description

Clear IPS policy log redundancy filter.

Options

filter Clear log redundancy filter in seconds.

Example

no log-redundancy filter

Syntax

priority { high | low | medium }

Mode

IPS Policy

Description

Set IPS policy priority.

Options

- high** High priority.
- low** Low priority.
- medium** Medium priority.

Example

priority high

Syntax

direction { both | incoming | outgoing } { to-client | to-server }

Mode

IPS Policy

Description

Set IPS policy direction.

Options

<i>both</i>	Both.
<i>incoming</i>	Incoming.
<i>outgoing</i>	Outgoing.
<i>to-client</i>	To client.
<i>to-server</i>	To server.

Example

```
direction both to-client
```

Syntax

```
no direction { both | incoming | outgoing } { to-client | to-server }
```

Mode

IPS Policy

Description

Clear IPS policy direction.

Options

<i>both</i>	Both.
<i>incoming</i>	Incoming.
<i>outgoing</i>	Outgoing.
<i>to-client</i>	To client.
<i>to-server</i>	To server.

Example

```
no direction both to-client
```

Syntax

```
gateway-antivirus
```

Mode

Config

Description

Enter Gateway Anti-Virus Configuration Mode.

Example

```
gateway-antivirus
```

Syntax

```
update-signatures
```

Mode

Gateway Anti-Virus

Description

Update signature database.

Example

update-signatures

Syntax

enable

Mode

Gateway Anti-Virus

Description

Enable Gateway Anti-Virus service.

Example

enable

Syntax

no enable

Mode

Gateway Anti-Virus

Description

Disable Gateway Anti-Virus service.

Example

no enable

Syntax

signature [enable] { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }

Mode

Gateway Anti-Virus

Description

Enable signature.

Options

<i>enable</i>	Enable signature.
<i>id</i>	Signature ID.
<i><GAV_SIG_ID></i>	Signature ID. Example: <i>1234</i>
<i>name</i>	Signature name.
<i><GAV_SIG_NAME></i>	Signature name. Example: <i>007SpySoft.G (Trojan)</i>

Example


```
signature name "180Solutions_6 (Adware)"
```

Syntax

```
no signature [ enable ] { id <GAV_SIG_ID> | name <GAV_SIG_NAME> }
```

Mode

Gateway Anti-Virus

Description

Disable signature.

Options

<i>enable</i>	Disable signature.
<i>id</i>	Signature ID.
<i><GAV_SIG_ID></i>	Signature ID. Example: <i>1234</i>
<i>name</i>	Signature name.
<i><GAV_SIG_NAME></i>	Signature name. Example: <i>007SpySoft.G (Trojan)</i>

Example

```
no signature name "180Solutions_6 (Adware)"
```

Syntax

```
inbound-inspection { cifs-netbios | ftp | http | imap | pop3 | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Enable inbound inspection for the specified protocols.

Options

<i>cifs-netbios</i>	CIFS/NetBIOS.
<i>ftp</i>	FTP.
<i>http</i>	HTTP.
<i>imap</i>	IMAP.
<i>pop3</i>	POP3.
<i>smtp</i>	SMTP.
<i>tcp-stream</i>	TCP Stream.

Example

```
inbound-inspection http
```

Syntax

```
no inbound-inspection { cifs-netbios | ftp | http | imap | pop3 | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Disable inbound inspection for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

tcp-stream TCP Stream.

Example

```
no inbound-inspection http
```

Syntax

```
outbound-inspection { ftp | http | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Enable outbound inspection for the specified protocols.

Options

ftp FTP.

http HTTP.

smtp SMTP.

tcp-stream TCP Stream.

Example

```
outbound-inspection http
```

Syntax

```
no outbound-inspection { ftp | http | smtp | tcp-stream }
```

Mode

Gateway Anti-Virus

Description

Disable outbound inspection for the specified protocols.

Options

<i>ftp</i>	FTP.
<i>http</i>	HTTP.
<i>smtp</i>	SMTP.
<i>tcp-stream</i>	TCP Stream.

Example

```
no outbound-inspection http
```

Syntax

```
restrict password-protected-zip { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of password-protected ZIP files for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
restrict password-protected-zip http
```

Syntax

```
no restrict password-protected-zip { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of password-protected ZIP files for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
no restrict password-protected-zip http
```

Syntax

```
restrict ms-office-macros { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of MS-Office type files containing macros (VBA 5 and above).

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
restrict ms-office-macros http
```

Syntax

```
no restrict ms-office-macros { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of MS-Office type files containing macros (VBA 5 and above) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
no restrict ms-office-macros http
```

Syntax

```
restrict packed-executables { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
restrict packed-executables http
```

Syntax

```
no restrict packed-executables { cifs-netbios | ftp | http | imap | pop3 | smtp }
```

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Options

cifs-netbios CIFS/NetBIOS.

ftp FTP.

http HTTP.

imap IMAP.

pop3 POP3.

smtp SMTP.

Example

```
no restrict packed-executables http
```

Syntax

```
exclusion-object http { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Address object group Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Address object name Address object name. Example: <i>Web Server</i>

Example

```
exclusion-object http name "WLAN Subnets"
```

Syntax

```
exclusion-object ftp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>

<ADDR_MASK>	Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Address object group
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion-object ftp name "WLAN Subnets"
```

Syntax

```
exclusion-object imap { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Address object group
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion-object imap name "WLAN Subnets"
```

Syntax

```
exclusion-object smtp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Address object group Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Address object name Address object name. Example: <i>Web Server</i>

Example

```
exclusion-object smtp name "WLAN Subnets"
```

Syntax

```
exclusion-object pop3 { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }  
| group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:

HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

network	Address object network.
<ADDR_NETWORK>	IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Address object group
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

exclusion-object pop3 name "WLAN Subnets"

Syntax

```
exclusion-object cifs-netbios { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN>  
<ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }
```

Mode

Gateway Anti-Virus

Description

Configure gateway AV protocol exclusion address objects.

Options

ipv6	Excluded IPv6 addresses.
host	Address object host.
<ADDR_HOST>	IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group	Address object group
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name

<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

exclusion-object cifs-netbios name "WLAN Subnets"

Syntax

no exclusion-object { cifs-netbios | ftp | http | imap | pop3 | smtp }

Mode

Gateway Anti-Virus

Description

Clear gateway AV protocol exclusion address objects.

Options

- cifs-netbios*** Clear CIFS/NetBIOS protocol exclusion address object.
- ftp*** Clear FTP protocol exclusion address object.
- http*** Clear HTTP protocol exclusion address object.
- imap*** Clear IMAP protocol exclusion address object.
- pop3*** Clear POP3 protocol exclusion address object.
- smtp*** Clear SMTP protocol exclusion address object.

Example

no exclusion-object http

Syntax

reset-settings

Mode

Gateway Anti-Virus

Description

Reset Gateway Anti-Virus Settings to default.

Example

reset-settings

Syntax

cloud anti-virus-database

Mode

Gateway Anti-Virus

Description

Enable Cloud Anti-Virus Database.

Example

Syntax

no cloud anti-virus-database

Mode

Gateway Anti-Virus

Description

Disable Cloud Anti-Virus Database.

Example

no cloud anti-virus-database

Syntax

cloud exclusion { id <UINT32> | name <GAV_SIG_NAME> }

Mode

Gateway Anti-Virus

Description

Add a Cloud Anti-Virus Database exclusion.

Options

id	Signature ID.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
name	Signature name.
<GAV_SIG_NAME>	Signature name. Example: 007SpySoft.G (Trojan)

Example

cloud exclusion id 1345342

Syntax

no cloud exclusion { id <UINT32> | name <GAV_SIG_NAME> }

Mode

Gateway Anti-Virus

Description

Remove a Cloud Anti-Virus Database exclusion.

Options

id	Signature ID.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
name	Signature name.
<GAV_SIG_NAME>	Signature name. Example: 007SpySoft.G (Trojan)

Example

```
no cloud exclusion id 1345342
```

Syntax

```
no cloud exclusions
```

Mode

Gateway Anti-Virus

Description

Delete all Cloud Anti-Virus Database exclusions.

Example

```
no cloud exclusions
```

Syntax

```
smtp-responses
```

Mode

Gateway Anti-Virus

Description

Enable SMTP responses.

Example

```
smtp-responses
```

Syntax

```
no smtp-responses
```

Mode

Gateway Anti-Virus

Description

Disable SMTP responses.

Example

```
no smtp-responses
```

Syntax

```
eicar-detection
```

Mode

Gateway Anti-Virus

Description

Enable detection of EICAR test virus.

Example

```
eicar-detection
```

Syntax

no eicar-detection

Mode

Gateway Anti-Virus

Description

Disable detection of EICAR test virus.

Example

no eicar-detection

Syntax

http-byte-range

Mode

Gateway Anti-Virus

Description

Enable HTTP Byte-Range requests with Gateway AV.

Example

http-byte-range

Syntax

no http-byte-range

Mode

Gateway Anti-Virus

Description

Disable HTTP Byte-Range requests with Gateway AV.

Example

no http-byte-range

Syntax

ftp-rest

Mode

Gateway Anti-Virus

Description

Enable FTP 'REST' requests with Gateway AV.

Example

ftp-rest

Syntax

no ftp-rest

Mode

Gateway Anti-Virus

Description

Disable FTP 'REST' requests with Gateway AV.

Example

no ftp-rest

Syntax

scan-high-compression

Mode

Gateway Anti-Virus

Description

Scan parts of files with high compression ratios.

Example

scan-high-compression

Syntax

no scan-high-compression

Mode

Gateway Anti-Virus

Description

Do not scan parts of files with high compression ratios.

Example

no scan-high-compression

Syntax

block-multiple-compress-files

Mode

Gateway Anti-Virus

Description

Enable to block files with multiple levels of zip/gzip compression.

Example

block-multiple-compress-files

Syntax

no block-multiple-compress-files

Mode

Gateway Anti-Virus

Description

Disable to block files with multiple levels of zip/gzip compression.

Example

```
no block-multiple-compress-files
```

Syntax

```
detection-only
```

Mode

Gateway Anti-Virus

Description

Enable detection only mode.

Example

```
detection-only
```

Syntax

```
no detection-only
```

Mode

Gateway Anti-Virus

Description

Disable detection only mode.

Example

```
no detection-only
```

Syntax

```
http-clientless-notification
```

Mode

Gateway Anti-Virus

Description

Enable HTTP Clientless Notification Alerts.

Example

```
http-clientless-notification
```

Syntax

```
no http-clientless-notification
```

Mode

Gateway Anti-Virus

Description

Disable HTTP Clientless Notification Alerts.

Example

no http-clientless-notification

Syntax

no notification-message

Mode

Gateway Anti-Virus

Description

Clear HTTP Clientless Notification Message to display when blocking.

Example

no notification-message

Syntax

notification-message <WORD>

Mode

Gateway Anti-Virus

Description

Set HTTP Clientless Notification Message to display when blocking.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

notification-message "This request is blocked by the SonicWall Gateway Anti-Virus Service."

Syntax

exclusion { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | address {
{ object | range } } | entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST> | group <ADDR_GROUP_NAME_MIXED> |
list | name <ADDR_NAME_MIXED> }

Mode

Gateway Anti-Virus

Description

Configure gateway AV exclusion list.

Options

ipv6	Excluded IPv6 addresses.
host	Address object host.
<ADDR_HOST>	IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:3257:9652\n

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
address	Set exclusion list method.
object	Set exclusion list with address object.
range	Set exclusion list with address range.
entry	Gateway AV exclusion list entry.
<GAV_EXCLUSION_BEGIN_IPV4_HOST>	Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
<GAV_EXCLUSION_END_IPV4_HOST>	Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
group	Address object group
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
list	Enable gateway AV exclusion list.
name	Address object name
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion list
exclusion name "WLAN Subnets"
exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
from <GAV_EXCLUSION_BEGIN_IPV4_HOST>
```

Mode

Gateway AV Exclusion Entry

Description

Set Gateway AV exclusion list entry start ip.

Options

<GAV_EXCLUSION_BEGIN_IPV4_HOST> Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D.
Example: *192.168.168.168*

Example

```
from 10.10.10.1
```

Syntax

```
to <GAV_EXCLUSION_END_IPV4_HOST>
```

Mode

Description

Set Gateway AV exclusion list entry end ip.

Options

<GAV_EXCLUSION_END_IPV4_HOST> Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D.
Example: *192.168.168.168*

Example

to 10.10.10.1

Syntax

```
no exclusion { entries | entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST> | list }
```

Mode

Gateway Anti-Virus

Description

Disable gateway AV exclusion list.

Options

entries Delete all gateway AV exclusion list entries.

entry Delete gateway AV exclusion list entry.

<GAV_EXCLUSION_BEGIN_IPV4_HOST> Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D.
Example: *192.168.168.168*

<GAV_EXCLUSION_END_IPV4_HOST> Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D.
Example: *192.168.168.168*

list Disable gateway AV exclusion list.

Example

```
no exclusion list
no exclusion entry 10.10.10.1 10.10.10.10
```

Syntax

```
capture-atp
```

Mode

Config

Description

Enter capture ATP mode and configure settings.

Example

```
capture-atp
```

Syntax

```
enable
```

Mode

Capture ATP

Description

Enable the capture ATP services.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Capture ATP

Description

Disable the capture ATP services.

Example

```
no enable
```

Syntax

```
location { cloud | local }
```

Mode

Capture ATP

Description

Select Capture ATP location.

Options

cloud Cloud.

local Local.

Example

```
location local
```

Syntax

```
local-name-or-ip <HOSTNAME>
```

Mode

Capture ATP

Description

Local Capture ATP name or ip address.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
local-name-or-ip 1.2.3.4
```

Syntax

```
no local-name-or-ip
```

Mode

Capture ATP

Description

Local Capture ATP name or ip address.

Example

```
local-name-or-ip 1.2.3.4
```

Syntax

```
file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Enable the file types that maybe transferred to capture ATP for analysis.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
file-type exe
file-type pdf
file-type office
file-type officex
file-type archives
```

Syntax

```
no file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Disable the file types that maybe transferred to capture ATP for analysis.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
no file-type exe
no file-type pdf
no file-type office
no file-type officex
no file-type archives
```

Syntax

```
file-size { default | restrict <UINT32> }
```

Mode

Capture ATP

Description

Specify the maximum file size that may be transferred to capture ATP for analysis.

Options

default Use the default file size specified by the capture service.

restrict Restrict to specific value in KB.

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
file-size default
file-size restrict 1000
```

Syntax

```
exclude address for-capture-atp { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Capture ATP

Description

Set an address object to exclude from capture ATP.

Options

ipv6	IPv6 address object.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

<ADDR_END>	Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

exclude address for-capture-atp name "X0 IP"

Syntax

no exclude address for-capture-atp

Mode

Capture ATP

Description

Clear the address object to exclude from capture ATP.

Example

no exclude address for-capture-atp

Syntax

exclude md5-entry <EXCLUDE_MD5_ENTRY>

Mode

Capture ATP

Description

Add an entry to the capture ATP MD5 exclusion list.

Options

<EXCLUDE_MD5_ENTRY> MD5 exclusion entry in 32 hexadecimal digits.
Example: *11223344556677889900aabbccddeeff*

Example

exclude md5-entry 11223344556677889900aabbccddeeff

Syntax

no exclude md5-entry <EXCLUDE_MD5_ENTRY>

Mode

Capture ATP

Description

Delete an entry from the capture ATP MD5 exclusion list.

Options

<EXCLUDE_MD5_ENTRY> MD5 exclusion entry in 32 hexadecimal digits.
Example: *11223344556677889900aabbccddeeff*

Example

```
no exclude md5-entry 11223344556677889900aabbccddeeff
```

Syntax

```
no exclude md5-entries
```

Mode

Capture ATP

Description

Clear the capture ATP MD5 exclusion list.

Example

```
no exclude md5-entries
```

Syntax

```
exclude http-entry <EXCLUDE_HTTP_ENTRY>
```

Mode

Capture ATP

Description

Add an entry to the capture ATP HTTP exclusion list.

Options

<EXCLUDE_HTTP_ENTRY> HTTP exclusion entry as a FQDN or an IP address.
Example: **.google.com*

Example

```
exclude http-entry *.google.com
```

Syntax

```
no exclude http-entry <EXCLUDE_HTTP_ENTRY>
```

Mode

Capture ATP

Description

Delete an entry from the capture ATP HTTP exclusion list.

Options

<EXCLUDE_HTTP_ENTRY> HTTP exclusion entry as a FQDN or an IP address.
Example: **.google.com*

Example

```
no exclude http-entry *.google.com
```

Syntax

```
no exclude http-entries
```

Mode

Capture ATP

Description

Clear the capture ATP HTTP exclusion list.

Example

```
no exclude http-entries
```

Syntax

```
await-verdict { allow | block }
```

Mode

Capture ATP

Description

Set the custom block behavior for files that are not identified as malicious by other security services on the firewall and will be sent to capture ATP cloud service.

Options

allow Allow file download while awaiting a verdict.

block Block file download until a verdict is returned.

Example

```
await-verdict allow
```

Syntax

```
exclude address for-block-until-verdict { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Capture ATP

Description

Set an address object to exclude from blocking the file download until verdict is reached by the capture service.

Options

ipv6	IPv6 address object.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>

<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclude address for-block-until-verdict name "X0 IP"
```

Syntax

```
no exclude address for-block-until-verdict
```

Mode

Capture ATP

Description

Clear the address object to exclude from blocking the file download until verdict is reached by the capture service.

Example

```
no exclude address for-block-until-verdict
```

Syntax

```
exclude file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Set the file types to exclude from blocking the file download until verdict is reached by the capture service.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
exclude file-type exe
exclude file-type pdf
exclude file-type office
exclude file-type officex
exclude file-type archives
```

Syntax

```
no exclude file-type { archives | exe | office | officex | pdf }
```

Mode

Capture ATP

Description

Clear the file types to exclude from blocking the file download until verdict is reached by the capture service.

Options

archives Archives (.jar, .apk, .rar, .gz, and .zip).

exe Executables (PE, Mach-O, and DMG).

office Office 97-2003(.doc , .xls ,...).

officex Office(.docx , .xlsx ,...).

pdf PDF.

Example

```
no exclude file-type exe
no exclude file-type pdf
no exclude file-type office
no exclude file-type officex
no exclude file-type archives
```

Syntax

```
test uftp-connectivity
```

Mode

Capture ATP

Description

Test UFTP Connectivity.

Example

```
test uftp-connectivity
```

Syntax

```
clear uftp-connectivity
```

Mode

Capture ATP

Description

Clear UFTP Connectivity.

Example

```
clear uftp-connectivity
```

Syntax

```
refresh uftp-connectivity
```

Mode

Capture ATP

Description

Refresh UFTP Connectivity.

Example

```
refresh uftp-connectivity
```

Syntax

```
check md5-query-status <EXCLUDE_MD5_ENTRY>
```

Mode

Capture ATP

Description

Check MD5 query status.

Options

<EXCLUDE_MD5_ENTRY> MD5 exclusion entry in 32 hexadecimal digits.
Example: *11223344556677889900aabbccddeeff*

Example

```
check md5-query-status
```

Syntax

```
clear md5-query-status
```

Mode

Capture ATP

Description

Clear MD5 query status.

Example

```
clear md5-query-status
```

Syntax

```
refresh md5-query-status
```

Mode

Capture ATP

Description

Refresh MD5 query status.

Example

```
refresh md5-query-status
```

Syntax

```
no match-object <MATCH_OBJ_NAME>
```

Mode

Config

Description

Delete a match object.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

```
no match-object "myMatchObject"
```

Syntax

```
no match-objects
```

Mode

Config

Description

Delete all match objects.

Example

```
no match-objects
```

Syntax

```
match-object <MATCH_OBJ_NAME>
```

Mode

Config

Description

Add/edit match object and enter configuration mode.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

```
match-object "Denied File Extensions"
```

Syntax

no type

Mode

Match Object

Example

no type

Syntax

type { activex-class-id | application-category-list | application-list | application-signature-list | custom | email-body | email-cc | email-from | email-size | email-subject | email-to | file-content | file-extension | file-name | ftp-command | ftp-command-value | http-cookie | http-host | http-referer | http-request-custom-header | http-response-custom-header | http-set-cookie | http-uri-content | http-url | http-user-agent | ips-signature-category-list | ips-signature-list | log-email-user | mime-custom-header | web-browser }

Mode

Match Object

Description

Match object type.

Options

activex-class-id	Active X class ID.
application-category-list	Application category list.
application-list	Application list.
application-signature-list	Application signature list.
custom	Custom object.
email-body	E-mail body.
email-cc	E-mail CC.
email-from	E-mail from.
email-size	E-mail size.
email-subject	E-mail subject.
email-to	E-mail to.
file-content	File content.
file-extension	File extension.
file-name	File name.
ftp-command	FTP command.
ftp-command-value	FTP command and value.
http-cookie	HTTP cookie.
http-host	Http host.
http-referer	HTTP referer.
http-request-custom-header	HTTP request custom header.

http-response-custom-header HTTP response custom header.

http-set-cookie HTTP set cookie.

http-uri-content HTTP URI content.

http-url HTTP URL.

http-user-agent Http user agent.

ips-signature-category-list IPS signature category list.

ips-signature-list IPS signature list.

log-email-user Log e-mail user.

mime-custom-header MIME custom header.

web-browser Web browser.

Example

type email-body

Syntax

name <MATCH_OBJ_NAME>

Mode

Match Object

Description

Set match object name.

Options

<MATCH_OBJ_NAME> Match object name.
Example: *Match FTP*

Example

name "Denied File Extensions "

Syntax

match-type { *exact* | *partial* | *prefix* | *regex* | *suffix* }

Mode

Match Object

Description

Set match object match type.

Options

exact Exact match.

partial Partial match.

prefix Prefix match.

regex Regular expression match.

suffix Suffix match.

Example

match-type exact

Syntax

no match-type

Mode

Match Object

Description

Clear match object match type.

Example

no match-type

Syntax

enable

Mode

Match Object

Description

Enable custom settings.

Example

enable

Syntax

no enable

Mode

Match Object

Description

Disable custom settings.

Example

no enable

Syntax

offset <UINT32>

Mode

Match Object

Description

Set offset.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

offset 1

Syntax

depth <UINT32>

Mode

Match Object

Description

Set depth.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

depth 1

Syntax

min-size <UINT32>

Mode

Match Object

Description

Set min size.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

min-size 1

Syntax

max-size <UINT32>

Mode

Match Object

Description

Set max size.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
max-size 1
```

Syntax

```
negative-matching
```

Mode

Match Object

Description

Enable negative matching.

Example

```
negative-matching
```

Syntax

```
no negative-matching
```

Mode

Match Object

Description

Disable negative matching.

Example

```
no negative-matching
```

Syntax

```
no input-representation
```

Mode

Match Object

Description

Clear match object input representation.

Example

```
no input-representation
```

Syntax

```
input-representation { alphanumeric | hexadecimal }
```

Mode

Match Object

Description

Set match object input representation.

Options

alphanumeric Alphanumeric.

hexadecimal Hexadecimal.

Example

input-representation alphanumeric

Syntax

content-entry <WORD>

Mode

Match Object

Description

Add match object content.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

content-entry mpg

Syntax

no content-entry <MATCH_OBJ_CONTENT_ENTRY>

Mode

Match Object

Description

Delete match object content.

Options

<MATCH_OBJ_CONTENT_ENTRY> Match object content.
Example: *mpg*

Example

no content-entry mpg

Syntax

no content-entries

Mode

Match Object

Description

Delete all match object content.

Example

no content-entries

Syntax

```
pre-defined-regex { aba-routing-number | amex-cc | canadian-sin | discover-cc | mastercard-cc | us-ssn | visa-cc }
```

Mode

Match Object

Description

Add a pre-defined regular expression.

Options

<i>aba-routing-number</i>	American bankers association (ABA) routing number.
<i>amex-cc</i>	American express credit card.
<i>canadian-sin</i>	Canadian social insurance number (SIN).
<i>discover-cc</i>	Discover card credit card.
<i>mastercard-cc</i>	Master card credit card.
<i>us-ssn</i>	United states social security number (SSN).
<i>visa-cc</i>	Visa credit card.

Example

```
pre-defined-regex visa-cc
```

Syntax

```
no pre-defined-regex { aba-routing-number | amex-cc | canadian-sin | discover-cc | mastercard-cc | us-ssn | visa-cc }
```

Mode

Match Object

Description

Remove a pre-defined regular expression.

Options

<i>aba-routing-number</i>	American bankers association (ABA) routing number.
<i>amex-cc</i>	American express credit card.
<i>canadian-sin</i>	Canadian social insurance number (SIN).
<i>discover-cc</i>	Discover card credit card.
<i>mastercard-cc</i>	Master card credit card.
<i>us-ssn</i>	United states social security number (SSN).
<i>visa-cc</i>	Visa credit card.

Example

```
no pre-defined-regex visa-cc
```

Syntax

```
browser { chrome | firefox | msie | netscape | safari }
```

Mode

Match Object

Description

Add match object browser.

Options

<i>chrome</i>	Chrome.
<i>firefox</i>	Firefox.
<i>msie</i>	Internet explorer.
<i>netscape</i>	Netscape.
<i>safari</i>	Safari.

Example

```
browser safari
```

Syntax

```
no browser { chrome | firefox | msie | netscape | safari }
```

Mode

Match Object

Description

Delete match object browser.

Options

<i>chrome</i>	Chrome.
<i>firefox</i>	Firefox.
<i>msie</i>	Internet explorer.
<i>netscape</i>	Netscape.
<i>safari</i>	Safari.

Example

```
no browser safari
```

Syntax

```
no browsers
```

Mode

Match Object

Description

Delete all match object browsers.

Example

no browsers

Syntax

custom-header <WORD>

Mode

Match Object

Description

Set custom header name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

custom-header "TBD "

Syntax

no custom-header

Mode

Match Object

Description

Clear custom header name.

Example

no custom-header

Syntax

email-size <UINT32>

Mode

Match Object

Description

Specify e-mail size in bytes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

email-size 1000000

Syntax

no email-size

Mode

Match Object

Description

Clear e-mail size.

Example

no email-size

Syntax

ftp-command { abort | account | allocate | append | ascii | binary | cd | cdup | delete | get | help | ls | mkdir | mode | modified-time | nlist | noop | passive | password | port | put | pwd | quit | reinitialize | rename-from | rename-to | restart | rmdir | site | size | status | structure | structure-mount | structure-unique | system | type | user }

Mode

Match Object

Description

Add match object FTP command.

Options

<i>abort</i>	ABORT.
<i>account</i>	ACCOUNT.
<i>allocate</i>	ALLOCATE.
<i>append</i>	APPEND.
<i>ascii</i>	ASCII.
<i>binary</i>	BINARY.
<i>cd</i>	CD.
<i>cdup</i>	CDUP.
<i>delete</i>	DELETE.
<i>get</i>	GET.
<i>help</i>	HELP.
<i>ls</i>	LS.
<i>mkdir</i>	MKDIR.
<i>mode</i>	MODE.
<i>modified-time</i>	MODIFIED_TIME.
<i>nlist</i>	NLIST.
<i>noop</i>	NOOP.
<i>passive</i>	PASSIVE.
<i>password</i>	PASSWORD.
<i>port</i>	PORT.
<i>put</i>	PUT.

<i>pwd</i>	PWD.
<i>quit</i>	QUIT.
<i>reinitialize</i>	REINITIALIZE.
<i>rename-from</i>	RENAME_FROM.
<i>rename-to</i>	RENAME_TO.
<i>restart</i>	RESTART.
<i>rmdir</i>	RMDIR.
<i>site</i>	SITE.
<i>size</i>	SIZE.
<i>status</i>	STATUS.
<i>structure</i>	STRUCTURE.
<i>structure-mount</i>	STRUCTURE_MOUNT.
<i>structure-unique</i>	STRUCTURE_UNIQUE.
<i>system</i>	SYSTEM.
<i>type</i>	TYPE.
<i>user</i>	USER.

Example

```
ftp-command put
```

Syntax

```
no ftp-command { abort | account | allocate | append | ascii | binary | cd | cdup | delete | get | help | ls | mkdir | mode |
modified-time | nlist | noop | passive | password | port | put | pwd | quit | reinitialize | rename-from | rename-to | restart
| rmdir | site | size | status | structure | structure-mount | structure-unique | system | type | user }
```

Mode

Match Object

Description

Delete match object FTP command.

Options

<i>abort</i>	ABORT.
<i>account</i>	ACCOUNT.
<i>allocate</i>	ALLOCATE.
<i>append</i>	APPEND.
<i>ascii</i>	ASCII.
<i>binary</i>	BINARY.
<i>cd</i>	CD.
<i>cdup</i>	CDUP.

<i>delete</i>	DELETE.
<i>get</i>	GET.
<i>help</i>	HELP.
<i>ls</i>	LS.
<i>mkdir</i>	MKDIR.
<i>mode</i>	MODE.
<i>modified-time</i>	MODIFIED_TIME.
<i>nlist</i>	NLIST.
<i>noop</i>	NOOP.
<i>passive</i>	PASSIVE.
<i>password</i>	PASSWORD.
<i>port</i>	PORT.
<i>put</i>	PUT.
<i>pwd</i>	PWD.
<i>quit</i>	QUIT.
<i>reinitialize</i>	REINITIALIZE.
<i>rename-from</i>	RENAME_FROM.
<i>rename-to</i>	RENAME_TO.
<i>restart</i>	RESTART.
<i>rmdir</i>	RMDIR.
<i>site</i>	SITE.
<i>size</i>	SIZE.
<i>status</i>	STATUS.
<i>structure</i>	STRUCTURE.
<i>structure-mount</i>	STRUCTURE_MOUNT.
<i>structure-unique</i>	STRUCTURE_UNIQUE.
<i>system</i>	SYSTEM.
<i>type</i>	TYPE.
<i>user</i>	USER.

Example

```
no ftp-command put
```

Syntax

no ftp-commands

Mode

Match Object

Description

Delete all match object FTP commands.

Example

no ftp-commands

Syntax

argument <WORD>

Mode

Match Object

Description

Add FTP command argument.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

argument file1

Syntax

no argument <MATCH_OBJ_CONTENT_ENTRY>

Mode

Match Object

Description

Delete FTP command argument.

Options

<MATCH_OBJ_CONTENT_ENTRY> Match object content.
Example: *mpg*

Example

no argument file1

Syntax

no arguments

Mode

Match Object

Description

Delete all FTP command arguments.

Example

no arguments

Syntax

```
ips category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> }
```

Mode

Match Object

Description

Add an IPS category.

Options

id	Category ID.
<IPS_CATEGORY_ID>	Category ID. Example: <i>1234</i>
name	Category name.
<IPS_CATEGORY_NAME>	Category name. Example: <i>ACTIVEX</i>

Example

```
ips category name ACTIVEX
```

Syntax

```
no ips category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> }
```

Mode

Match Object

Description

Delete an IPS category.

Options

id	Category ID.
<IPS_CATEGORY_ID>	Category ID. Example: <i>1234</i>
name	Category name.
<IPS_CATEGORY_NAME>	Category name. Example: <i>ACTIVEX</i>

Example

```
no ips category name ACTIVEX
```

Syntax

```
no ips categories
```

Mode

Match Object

Description

Delete all IPS categories.

Example

no ips categories

Syntax

ips policy category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } signature { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> }

Mode

Match Object

Description

Add an IPS policy.

Options

<i>category</i>	Category.
<i>id</i>	Category ID.
<i><IPS_CATEGORY_ID></i>	Category ID. Example: <i>1234</i>
<i>name</i>	Category name.
<i><IPS_CATEGORY_NAME></i>	Category name. Example: <i>ACTIVEX</i>
<i>signature</i>	Signature.
<i>id</i>	Signature ID.
<i><IPS_POLICY_ID></i>	Policy ID. Example: <i>1234</i>
<i>name</i>	Signature name.
<i><IPS_POLICY_NAME></i>	Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i>

Example

ips category name ACTIVEX signature name "Free Tetris Executable (Adware)"

Syntax

no ips policy category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } signature { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> }

Mode

Match Object

Description

Delete an IPS policy.

Options

<i>category</i>	Category.
<i>id</i>	Category ID.
<i><IPS_CATEGORY_ID></i>	Category ID. Example: <i>1234</i>
<i>name</i>	Category name.
<i><IPS_CATEGORY_NAME></i>	Category name. Example: <i>ACTIVEX</i>
<i>signature</i>	Signature.
<i>id</i>	Signature ID.

<IPS_POLICY_ID>	Policy ID. Example: <i>1234</i>
name	Signature name.
<IPS_POLICY_NAME>	Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i>

Example

```
no ips category name ACTIVEX signature name "Free Tetris Executable (Adware)"
```

Syntax

```
no ips policies
```

Mode

Match Object

Description

Delete all IPS policies.

Example

```
no ips policies
```

Syntax

```
category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> }
```

Mode

Match Object

Description

Add an application category.

Options

id	Category ID.
<AC_CATEGORY_ID>	Category ID. Example: <i>123</i>
name	Category name.
<AC_CATEGORY_NAME>	Category name. Example: <i>APP-UPDATE</i>

Example

```
category name APP-UPDATE
category id 22
```

Syntax

```
no category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> }
```

Mode

Match Object

Description

Delete an application category.

Options

<i>id</i>	Category ID.
<i><AC_CATEGORY_ID></i>	Category ID. Example: <i>123</i>
<i>name</i>	Category name.
<i><AC_CATEGORY_NAME></i>	Category name. Example: <i>APP-UPDATE</i>

Example

```
no category name APP-UPDATE
no category id 22
```

Syntax

```
no categories
```

Mode

Match Object

Description

Delete all application categories.

Example

```
no categories
```

Syntax

```
application category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> }
```

Mode

Match Object

Description

Add an application.

Options

<i>category</i>	Application category.
<i>id</i>	Category ID.
<i><AC_CATEGORY_ID></i>	Category ID. Example: <i>123</i>
<i>name</i>	Category name.
<i><AC_CATEGORY_NAME></i>	Category name. Example: <i>APP-UPDATE</i>
<i>app</i>	Application.
<i>id</i>	Application ID.
<i><AC_APP_ID></i>	Application ID. Example: <i>123</i>
<i>name</i>	Application name.
<i><AC_APP_NAME></i>	Application name. Example: <i>APP-UPDATE</i>

Example

```
application category name BACKUP-APPS app name Dropbox
application category id 56 app id 604
```

Syntax

```
no application category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> }
```

Mode

Match Object

Description

Delete an application.

Options

category	Application category.
id	Category ID.
<AC_CATEGORY_ID>	Category ID. Example: 123
name	Category name.
<AC_CATEGORY_NAME>	Category name. Example: APP-UPDATE
app	Application.
id	Application ID.
<AC_APP_ID>	Application ID. Example: 123
name	Application name.
<AC_APP_NAME>	Application name. Example: APP-UPDATE

Example

```
no application category name BACKUP-APPS app name Dropbox
no application category id 56 app id 604
```

Syntax

```
no applications
```

Mode

Match Object

Description

Delete all applications.

Example

```
no applications
```

Syntax

```
signature category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> } sig { id <AC_SIG_ID> | name <AC_SIG_NAME> }
```

Mode

Match Object

Description

Add a signature.

Options

category	Application category.

<i>id</i>	Category ID.
<i><AC_CATEGORY_ID></i>	Category ID. Example: <i>123</i>
<i>name</i>	Category name.
<i><AC_CATEGORY_NAME></i>	Category name. Example: <i>APP-UPDATE</i>
<i>app</i>	Application.
<i>id</i>	Application ID.
<i><AC_APP_ID></i>	Application ID. Example: <i>123</i>
<i>name</i>	Application name.
<i><AC_APP_NAME></i>	Application name. Example: <i>APP-UPDATE</i>
<i>sig</i>	Signature.
<i>id</i>	Signature ID.
<i><AC_SIG_ID></i>	Signature ID. Example: <i>123</i>
<i>name</i>	Signature name.
<i><AC_SIG_NAME></i>	Signature name.

Example

```
signature category name BACKUP-APPS app name Dropbox sig name "SSL Traffic"
signature category id 56 app id 604 sig id 1736
```

Syntax

```
no signature category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } app { id <AC_APP_ID> | name <AC_APP_NAME> } sig { id <AC_SIG_ID> | name <AC_SIG_NAME> }
```

Mode

Match Object

Description

Delete a signature.

Options

<i>category</i>	Application category.
<i>id</i>	Category ID.
<i><AC_CATEGORY_ID></i>	Category ID. Example: <i>123</i>
<i>name</i>	Category name.
<i><AC_CATEGORY_NAME></i>	Category name. Example: <i>APP-UPDATE</i>
<i>app</i>	Application.
<i>id</i>	Application ID.
<i><AC_APP_ID></i>	Application ID. Example: <i>123</i>
<i>name</i>	Application name.
<i><AC_APP_NAME></i>	Application name. Example: <i>APP-UPDATE</i>
<i>sig</i>	Signature.
<i>id</i>	Signature ID.
<i><AC_SIG_ID></i>	Signature ID. Example: <i>123</i>
<i>name</i>	Signature name.
<i><AC_SIG_NAME></i>	Signature name.

Example

```
no signature category name BACKUP-APPS app name Dropbox sig name "SSL Traffic"
no signature category id 56 app id 604 sig id 1736
```

Syntax

```
no signatures
```

Mode

Match Object

Description

Delete all signatures.

Example

```
no signatures
```

Syntax

```
action-object <ACTION_OBJ_NAME>
```

Mode

Config

Description

Create/edit specified action object and enter its configuration mode.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

```
action-object "Corp E-mail Message"
```

Syntax

```
no action-object <ACTION_OBJ_NAME>
```

Mode

Config

Description

Delete specified action object.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

```
no action-object "Corp E-mail Message"
```

Syntax

no action-objects

Mode

Config

Description

Delete all action objects.

Example

no action-objects

Syntax

name <ACTION_OBJ_NAME>

Mode

Action Object

Description

Action object name.

Options

<ACTION_OBJ_NAME> Action object name.
Example: *HTTP Block Page*

Example

name "Corp Mail Message"

Syntax

action { *bandwidth-management* | *block-smtp-error-reply* | *disable-email-attachment* | *email-add-text* | *ftp-notification-reply* | *http-block-page* | *http-redirect* }

Mode

Action Object

Description

Set action.

Options

<i>bandwidth-management</i>	Bandwidth management.
<i>block-smtp-error-reply</i>	Block SMTP e-mail and send error reply.
<i>disable-email-attachment</i>	Disable e-mail attachment and add text.
<i>email-add-text</i>	E-mail - add text.
<i>ftp-notification-reply</i>	FTP notification reply.
<i>http-block-page</i>	HTTP block page.
<i>http-redirect</i>	HTTP redirect.

Example

action block-smtp-email error-reply

Syntax

no content

Mode

Action Object

Description

Clear action object content.

Example

no content

Syntax

content <WORD>

Mode

Action Object

Description

Action object content.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

content "Corporate does not allow attachments to Emails."

Syntax

no color

Mode

Action Object

Description

Clear HTTP block page color.

Example

no color

Syntax

color { blue | red | white | yellow }

Mode

Action Object

Description

HTTP block page color.

Options

blue Blue.

red Red.

white White.

yellow Yellow.

Example

`color white`

Syntax

`bandwidth-management`

Mode

Action Object

Description

Configure bandwidth management.

Example

`bandwidth-management`

Syntax

`aggregation-method { per-action | per-policy }`

Mode

Bandwidth Management

Description

Set the bandwidth aggregation method.

Options

per-action Per action.

per-policy Per policy.

Example

`aggregation-method per-policy`

Syntax

`no egress [ bandwidth-object ]`

Mode

Bandwidth Management

Description

Disable egress bandwidth management.

Options

bandwidth-object Clear bandwidth object.

Example

no egress

Syntax

egress bandwidth-object <BANDWIDTH_RULE_NAME>

Mode

Bandwidth Management

Description

Enable egress bandwidth management and configure.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\ "Corp High Priority\"`

Example

egress bandwidth-object "Corp High Priority"

Syntax

no ingress [*bandwidth-object*]

Mode

Bandwidth Management

Description

Disable ingress bandwidth management.

Options

bandwidth-object Clear bandwidth object.

Example

no ingress

Syntax

ingress bandwidth-object <BANDWIDTH_RULE_NAME>

Mode

Bandwidth Management

Description

Enable ingress bandwidth management and configure.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\ "Corp High Priority\"`

Example

ingress bandwidth-object "Corp High Priority"

Syntax

usage-tracking

Mode

Bandwidth Management

Description

Enable tracking bandwidth usage.

Example

usage-tracking

Syntax

no usage-tracking

Mode

Bandwidth Management

Description

Disable tracking bandwidth usage.

Example

no usage-tracking

Syntax

no email-object <EMAIL_OBJ_NAME>

Mode

Config

Description

Delete an e-mail address object.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

no email-object "Client E-mail Addresses"

Syntax

no email-objects

Mode

Config

Description

Delete all e-mail address objects.

Example

no email-objects

Syntax

```
email-object <EMAIL_OBJ_NAME>
```

Mode

Config

Description

Add/edit e-mail address object and enter configuration mode.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

```
email-object "Client E-mail Addresses"
```

Syntax

```
name <EMAIL_OBJ_NAME>
```

Mode

E-mail Address Object

Description

Set e-mail address object name.

Options

<EMAIL_OBJ_NAME> E-mail object name.
Example: *Marketing E-mail Object*

Example

```
name "Client E-mail Addresses "
```

Syntax

```
no match-type
```

Mode

E-mail Address Object

Description

Clear e-mail address object match type.

Example

```
no match-type
```

Syntax

```
match-type { exact | partial | regex }
```

Mode

E-mail Address Object

Description

Set e-mail address object match type.

Options

- exact*** Exact match.
- partial*** Partial match.
- regex*** Regular expression match.

Example

```
match-type exact
```

Syntax

```
content-entry <EMAIL_OBJ_CONTENT_ENTRY>
```

Mode

E-mail Address Object

Description

Add e-mail address object content entry.

Options

- <EMAIL_OBJ_CONTENT_ENTRY>*** E-mail object content.
Example: *administrator@corp.local*

Example

```
content-entry administrator@corp.local
```

Syntax

```
no content-entry <EMAIL_OBJ_CONTENT_ENTRY>
```

Mode

E-mail Address Object

Description

Delete e-mail address object content entry.

Options

- <EMAIL_OBJ_CONTENT_ENTRY>*** E-mail object content.
Example: *administrator@corp.local*

Example

```
no content-entry administrator@corp.local
```

Syntax

```
no content-entries
```

Mode

E-mail Address Object

Description

Delete all e-mail address object content entries.

Example

no content-entries

Syntax

app-rules

Mode

Config

Description

Enter app rules configuration mode.

Example

app-rules

Syntax

enable

Mode

App Rules

Description

Enable app rules.

Example

enable

Syntax

no enable

Mode

App Rules

Description

Disable app rules.

Example

no enable

Syntax

log-redundancy <UINT32>

Mode

App Rules

Description

Set the global log redundancy filter interval(seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: 123

Example

```
log-redundancy 60
```

Syntax

```
no log-redundancy
```

Mode

App Rules

Description

Clear the global log redundancy filter interval.

Example

```
no log-redundancy
```

Syntax

```
no policy <APP_RULES_POLICY_NAME>
```

Mode

App Rules

Description

Delete specified app rule policy.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no policy "Deny Sensitive Download"
```

Syntax

```
no policies
```

Mode

App Rules

Description

Delete all app rule policies.

Example

```
no policies
```

Syntax

```
policy <APP_RULES_POLICY_NAME>
```

Mode

App Rules

Description

Create/edit specified app rule policy and enter its configuration mode.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

policy "Deny Sensitive Download"

Syntax

name <APP_RULES_POLICY_NAME>

Mode

App Rules Policy

Description

App rule name.

Options

<APP_RULES_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Deny Sensitive Emails"

Syntax

type { app-control | cfs | custom | ftp { { client | client-download | client-upload | data-transfer } } | http { { client | server } } | ips | pop3 { { client | server } } | smtp-client }

Mode

App Rules Policy

Description

Set app rule policy type.

Options

<i>app-control</i>	App control content.
<i>cfs</i>	CFS.
<i>custom</i>	Custom policy.
<i>ftp</i>	FTP.
<i>client</i>	FTP client.
<i>client-download</i>	FTP client file download.
<i>client-upload</i>	FTP client file upload.
<i>data-transfer</i>	FTP data transfer.
<i>http</i>	HTTP.
<i>client</i>	HTTP client.
<i>server</i>	HTTP server.

<i>ips</i>	IPS content.
<i>pop3</i>	POP3.
<i>client</i>	Pop3 client.
<i>server</i>	Pop3 server.
<i>smtp-client</i>	SMTP client.

Example

```
type http client
```

Syntax

```
source address { { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }
```

Mode

App Rules Policy

Description

Set the source address for the app rule policy.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i> <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>any</i>	Any address.
<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
<i>mac</i> <ADDR_MAC>	Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i> <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

source address name "Corporate IT Administration"

Syntax

destination address { { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }

Mode

App Rules Policy

Description

Set the destination address for the app rule policy.

Options

ipv6	IPv6 address object.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
mac <ADDR_MAC>	Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

destination address name "Corporate IT Administration"

Syntax

address { { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }

Mode

App Rules Policy

Description

Set the address for the app rule policy.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i> <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i> <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>any</i>	Any address.
<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
<i>mac</i> <ADDR_MAC>	Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i> <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

address name "Corporate IT Administration"

Syntax

exclusion address { { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } } | any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }

Mode

App Rules Policy

Description

Set the exclusion address for the app rule policy.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion address name "Corporate IT Administration"
```

Syntax

```
no exclusion address
```

Mode

App Rules Policy

Description

Clear exclusion address for the app rule policy.

Example

```
no exclusion address
```

Syntax

```
source service { any | name <APP_RULES_POLICY_SVC_NAME> }
```

Mode

App Rules Policy

Description

Set the source service for the app rule policy.

Options

any	Any source service.

<i>name</i>	Source service object name.
<i><APP_RULES_POLICY_SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>

Example

source service name "IT Maintenance"

Syntax

destination service { any | name <APP_RULES_POLICY_SVC_NAME> }

Mode

App Rules Policy

Description

Set the destination service for the app rule policy.

Options

<i>any</i>	Any destination service.
<i>name</i>	Destination service object name.
<i><APP_RULES_POLICY_SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>

Example

destination service name "Corporate Servers"

Syntax

match-object { excluded <APP_RULES_POLICY_MATCH_OBJECT> | included <APP_RULES_POLICY_MATCH_OBJECT> | object <APP_RULES_POLICY_MATCH_OBJECT> }

Mode

App Rules Policy

Description

Set match object for this app rule policy.

Options

<i>excluded</i>	Exclude match object.
<i><APP_RULES_POLICY_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>included</i>	Include match object.
<i><APP_RULES_POLICY_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>object</i>	Include match object.
<i><APP_RULES_POLICY_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

match-object object "mpg extension"

Syntax

action-object <APP_RULES_POLICY_ACTION_OBJECT>

Mode

App Rules Policy

Description

Set action object for this app rule policy.

Options

<APP_RULES_POLICY_ACTION_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

action-object "Bypass DPI"

Syntax

users { excluded | included } { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

App Rules Policy

Description

Set users to this app rule policy.

Options

- excluded* Set excluded users.
- included* Set included users.
- administrator* Administrator.
- all* All users.
- group* Group object name.
<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*
- guests* Guest users.
- name* User object name.
<LOCAL_USER_NAME> Local user object name.
Example: *user1*

Example

users included name "Corporate IT Administrators"

Syntax

no users excluded

Mode

App Rules Policy

Description

Clear excluded users for the app rule policy.

Options

excluded Clear excluded users for the app rule policy.

Example

no users excluded

Syntax

mail-from included <APP_RULES_POLICY_EMAIL_OBJECT>

Mode

App Rules Policy

Description

Set the included from e-mail object for the app rules policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

mail-from included any mail-from included "John Doe"

Syntax

mail-from excluded <APP_RULES_POLICY_EMAIL_OBJECT>

Mode

App Rules Policy

Description

Set the excluded from e-mail object for the app rules policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

mail-from excluded "Jane Doe"

Syntax

no mail-from excluded

Mode

App Rules Policy

Description

Clear the excluded from e-mail object for the app rules policy.

Options

excluded Clear the excluded from e-mail object for the app rules policy.

Example

no mail-from excluded

Syntax

```
rcpt-to included <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the included RCPT to e-mail address object for the app rule policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
rcpt-to included any rcpt-to included "John Doe"
```

Syntax

```
rcpt-to excluded <APP_RULES_POLICY_EMAIL_OBJECT>
```

Mode

App Rules Policy

Description

Set the excluded RCPT to e-mail address object for the app rule policy.

Options

<APP_RULES_POLICY_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
rcpt-to excluded "Jane Doe"
```

Syntax

```
no rcpt-to excluded
```

Mode

App Rules Policy

Description

Clear the excluded RCPT to e-mail object for the app rules policy.

Options

excluded Clear the excluded RCPT to e-mail object for the app rules policy.

Example

```
no rcpt-to excluded
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Rules Policy

Description

Specify a schedule for this app rule policy.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "IT Maintenance"

Syntax

enable

Mode

App Rules Policy

Description

Enable app rule policy.

Example

enable

Syntax

no enable

Mode

App Rules Policy

Description

Disable app rule policy.

Example

no enable

Syntax

flow-reporting

Mode

App Rules Policy

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

App Rules Policy

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

logging

Mode

App Rules Policy

Description

Enable logging when this app rule is used.

Example

logging

Syntax

no logging

Mode

App Rules Policy

Description

Disable logging when this app rule is used.

Example

no logging

Syntax

log individual

Mode

App Rules Policy

Description

Enable log individual object content.

Example

log individual

Syntax

no log individual

Mode

App Rules Policy

Description

Disable log individual object content.

Example

no log individual

Syntax

ips-message-format

Mode

App Rules Policy

Description

Enable log using IPS message format.

Example

ips-message-format

Syntax

no ips-message-format

Mode

App Rules Policy

Description

Disable log using IPS message format.

Example

no ips-message-format

Syntax

app-control-message-format

Mode

App Rules Policy

Description

Enable log using app control message format.

Example

app-control-message-format

Syntax

no app-control-message-format

Mode

App Rules Policy

Description

Disable log using app control message format.

Example

no app-control-message-format

Syntax

cfs-message-format

Mode

App Rules Policy

Description

Enable log using CFS message format.

Example

cfs-message-format

Syntax

no cfs-message-format

Mode

App Rules Policy

Description

Disable log using CFS message format.

Example

no cfs-message-format

Syntax

log redundancy { global | interval <UINT32> }

Mode

App Rules Policy

Description

Set log redundancy filter interval.

Options

global Use the global app rules redundancy filter setting.

interval Set the redundancy interval in seconds.

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
log-redundancy global
log-redundancy interval 60
```

Syntax

```
no log redundancy interval
```

Mode

App Rules Policy

Description

Clear log redundancy filter interval.

Options

interval Set the redundancy interval in seconds.

Example

```
no log redundancy interval
```

Syntax

```
connection-side { both | client | server }
```

Mode

App Rules Policy

Description

Set connection side.

Options

both Both sides.

client Client side.

server Server side.

Example

```
connection-side server
```

Syntax

```
direction { advanced [ [ from { any | zone <APP_RULES_POLICY_ZONE> } ] ] [ [ to { any | zone <APP_RULES_POLICY_ZONE> } ] ] ] |
basic [ [ both | incoming | outgoing ] ] }
```

Mode

App Rules Policy

Description

Set direction.

Options

advanced Advanced.

from From.

any	From any zone.
zone	Set the source zone.
<APP_RULES_POLICY_ZONE>	Zone object name. Example: <i>DMZ</i>
to	To.
any	To any zone.
zone	Set the destination zone.
<APP_RULES_POLICY_ZONE>	Zone object name. Example: <i>DMZ</i>
basic	Basic.
both	Both directions.
incoming	Incoming.
outgoing	Outgoing.

Example

direction incoming

Syntax

zone { any | name <APP_RULES_POLICY_ZONE> }

Mode

App Rules Policy

Description

Set zone.

Options

any	Set zone as any.
name	Set zone name.
<APP_RULES_POLICY_ZONE>	Zone object name. Example: <i>DMZ</i>

Example

zone any
zone name LAN

Syntax

cfs-list allow <APP_RULES_POLICY_CFS_LIST>

Mode

App Rules Policy

Description

Set CFS allow/included list for this app rules policy.

Options

<APP_RULES_POLICY_CFS_LIST>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
cfs-list allow "CFSAllowList"
```

Syntax

```
no cfs-list allow
```

Mode

App Rules Policy

Description

Clear CFS allow/included list for the app rules policy.

Example

```
no cfs-list allow
```

Syntax

```
cfs-list forbidden <APP_RULES_POLICY_CFS_LIST>
```

Mode

App Rules Policy

Description

Set CFS forbidden/excluded list for this app rules policy.

Options

<APP_RULES_POLICY_CFS_LIST> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
cfs-list forbidden "CFSForbiddenList"
```

Syntax

```
no cfs-list forbidden
```

Mode

App Rules Policy

Description

Clear CFS forbidden/excluded list for the app rules policy.

Example

```
no cfs-list forbidden
```

Syntax

```
safe-search
```

Mode

App Rules Policy

Description

Enable safe search enforcement.

Example

safe-search

Syntax

no safe-search

Mode

App Rules Policy

Description

Disable safe search enforcement.

Example

no safe-search

Syntax

youtube-for-schools

Mode

App Rules Policy

Description

Enable YouTube for schools.

Example

youtube-for-schools

Syntax

no youtube-for-schools

Mode

App Rules Policy

Description

Disbale YouTube for schools.

Example

no youtube-for-schools

Syntax

school-id <WORD>

Mode

App Rules Policy

Description

Set CFS school id.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

school-id HUST

Syntax

no school-id

Mode

App Rules Policy

Description

Clear CFS school id.

Example

no school-id

Syntax

app-control

Mode

Config

Description

Enter app control configuration mode.

Example

app-control

Syntax

update-signatures

Mode

App Control

Description

Update signature database.

Example

update-signatures

Syntax

enable

Mode

App Control

Description

Enable app control.

Example

enable

Syntax

no enable

Mode

App Control

Description

Disable app control.

Example

no enable

Syntax

log-all

Mode

App Control

Description

Enable logging for all apps.

Example

log-all

Syntax

no log-all

Mode

App Control

Description

Disable logging for all apps.

Example

no log-all

Syntax

log-filename

Mode

App Control

Description

Enable filename logging.

Example

log-filename

Syntax

no log-filename

Mode

App Control

Description

Disable filename logging.

Example

no log-filename

Syntax

log-redundancy filter <UINT16>

Mode

App Control

Description

Set app control log redundancy filter.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

App Control

Description

Clear app control log redundancy filter.

Example

no log-redundancy filter

Syntax

reset

Mode

App Control

Description

Reset app control settings to default.

Example

reset

Syntax

```
category { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } [ [ application { id <AC_APP_ID> | name <AC_APP_NAME> } [ signature { id <AC_SIG_ID> | name <AC_SIG_NAME> } ] ] ]
```

Mode

App Control

Description

Enter configuration mode for the specified app control category, application or signature.

Options

id	Category ID.
<AC_CATEGORY_ID>	Category ID. Example: <i>123</i>
name	Category name.
<AC_CATEGORY_NAME>	Category name. Example: <i>APP-UPDATE</i>
application	Enter configuration mode for the specified app control application.
id	Application ID.
<AC_APP_ID>	Application ID. Example: <i>123</i>
name	Application name.
<AC_APP_NAME>	Application name. Example: <i>APP-UPDATE</i>
signature	Enter configuration mode for the specified app control signature.
id	Signature ID.
<AC_SIG_ID>	Signature ID. Example: <i>123</i>
name	Signature name.
<AC_SIG_NAME>	Signature name.

Example

```
category name "GAMING"  
category name GAMING application name "Build-A-Bearville Online"  
category name APP-UPDATE application name 360Safe signature name "Update Traffic 6"
```

Syntax

```
exclusion list { ips | object { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } }
```

Mode

App Control

Description

Enable and configure application control exclusion list.

Options

ips	Use IPS exclusion list.
object	Use specified address object for exclusion list.

<i>ipv6</i>	IPv6 address.
<i>host</i>	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i>	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Specify IP range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>group</i>	Address object group.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
<i>name</i>	Specify name of address object.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclusion list ips
exclusion list object name "Corp App Control Exclusion List"
exclusion list object range 10.10.10.1 10.10.10.10
```

Syntax

```
no exclusion list
```

Mode

App Control

Description

Disable application control exclusion list.

Example

```
no exclusion list
```

Syntax

```
name <WORD>
```

Mode

App Control Category
App Control Application
App Control Signature

Description

Policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name GAMING

Syntax

id <UINT32>

Mode

App Control Category
App Control Application
App Control Signature

Description

Policy ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

id 8

Syntax

block

Mode

App Control Category

Description

Set blocking for app control category.

Example

block

Syntax

no block

Mode

App Control Category

Description

Disable blocking for app control category.

Example

no block

Syntax

log [enable | global]

Mode

App Control Category

Description

Set logging for app control category.

Options

enable Enable app control category logging.

global Use global setting.

Example

log global

Syntax

no log

Mode

App Control Category

Description

Disable logging for app control category.

Example

no log

Syntax

included users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

App Control Category

Description

Set included users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>all</i>	All.
<i>group</i> <i><LOCAL_USER_GROUP_NAME></i>	Specify local user group. Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.
<i>name</i> <i><LOCAL_USER_NAME></i>	Specify local user. Local user object name. Example: <i>user1</i>

Example

included users all

Syntax

excluded users { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

App Control Category

Description

Set excluded users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>group</i>	Specify local user group.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.
<i>name</i>	Specify local user.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

excluded users guests

Syntax

included ip { all | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

App Control Category

Description

Set included IP address range.

Options

<i>all</i>	All.
<i>group</i>	Address object group.
<i><ADDR_GROUP_NAME_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Specify name of range address object.
<i><ADDR_NAME_MIXED></i>	Address object name. Example: <i>Web Server</i>
<i>network</i>	Address object network.
<i><ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Specify IP range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Category

Description

Set excluded IP address range.

Options

group <ADDR_GROUP_NAME_MIXED>	Address object group. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_NAME_MIXED>	Specify name of range address object. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Specify IP range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Category

Description

Disable exclude users/groups or IP addresses.

Options

ip	Disable exclude IP addresses.
users	Disable exclude users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Category

Description

Set app control category schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule always-on
```

Syntax

```
log-redundancy { filter <UINT16> | global }
```

Mode

App Control Category

Description

Set app control category log redundancy filter.

Options

<i>filter</i>	Set log redundancy filter in seconds.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>global</i>	Use global setting.

Example

```
log-redundancy filter 45
```

Syntax

```
no log-redundancy filter
```

Mode

App Control Category

Description

Clear app control category log redundancy filter.

Options

filter Clear log redundancy filter.

Example

```
no log-redundancy filter
```

Syntax

```
block [ category | enable ]
```

Mode

App Control Application

Description

Set blocking for app control application.

Options

category Use category setting.

enable Enable app control application blocking.

Example

```
block category
```

Syntax

```
no block
```

Mode

App Control Application

Description

Disable blocking for app control application.

Example

```
no block
```

Syntax

```
log [ category | enable ]
```

Mode

App Control Application

Description

Set logging for app control application.

Options

- category** Use category setting.
- enable** Enable app control application logging.

Example

```
log category
```

Syntax

```
no log
```

Mode

App Control Application

Description

Disable logging for app control application.

Example

```
no log
```

Syntax

```
included users { administrator | all | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Application

Description

Set included users/groups.

Options

- administrator** Built-in administrator.
- all** All.
- category** Use category setting.
- group** Specify local user group.
<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*
- guests** Guests.
- name** Specify local user.
<LOCAL_USER_NAME> Local user object name.
Example: *user1*

Example

```
included users all
```

Syntax

```
excluded users { administrator | category | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

App Control Application

Description

Set excluded users/groups.

Options

<i>administrator</i>	Built-in administrator.
<i>category</i>	Use category setting.
<i>group</i>	Specify local user group.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests.
<i>name</i>	Specify local user.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

excluded users guests

Syntax

included ip { all | category | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

App Control Application

Description

Set included IP address range.

Options

<i>all</i>	All.
<i>category</i>	Use category setting.
<i>group</i>	Address object group.
<i><ADDR_GROUP_NAME></i>	Group address object name. Example: <i>Sales Group</i>
<i>host</i>	Address object host.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<i><ADDR_NAME_MIXED></i>	Address object name. Example: <i>Web Server</i>
<i>network</i>	Address object network.
<i><ADDR_NETWORK></i>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<i><ADDR_MASK></i>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Address object range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
included ip range 10.10.10.1 10.10.10.10
```

Syntax

```
excluded ip { category | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK>
<ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

App Control Application

Description

Set excluded IP address range.

Options

category	Use category setting.
group <ADDR_GROUP_NAME>	Address object group. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Application

Description

Disable exclude users/groups or IP addresses.

Options

ip	Disable exclude IP addresses.

users Disable exclude users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | category | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Application

Description

Set app control application schedule.

Options

always-on	Always on.
category	Use category setting.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule always-on
```

Syntax

```
log-redundancy { category | filter <UINT16> }
```

Mode

App Control Application

Description

Set app control application log redundancy filter.

Options

category	Use category setting.
filter	Set log redundancy filter in seconds.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
log-redundancy filter 45
```

Syntax

```
no log-redundancy filter
```

Mode

App Control Application

Description

Clear app control application log redundancy filter.

Options

filter Set log redundancy filter in seconds.

Example

```
no log-redundancy filter
```

Syntax

```
category <WORD>
```

Mode

App Control Signature
App Control Application

Description

App control signature or application's category name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
category WEBMAIL
```

Syntax

```
application <WORD>
```

Mode

App Control Signature

Description

App control signature's application name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
application Cox
```

Syntax

```
block [ app | enable ]
```

Mode

Description

Set blocking for app control signature.

Options

- app** Use app setting.
- enable** Enable app control signature blocking.

Example

block app

Syntax

no block

Mode

Description

Disable blocking for app control signature.

Example

no block

Syntax

log [app | enable]

Mode

Description

Set logging for app control signature.

Options

- app** Use app setting.
- enable** Enable app control signature logging.

Example

log app

Syntax

no log

Mode

Description

Disable logging for app control signature.

Example

no log

Syntax

included users { administrator | all | app | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

App Control Signature

Description

Set included users/groups.

Options

administrator	Built-in administrator.
all	All.
app	Use app setting.
group <LOCAL_USER_GROUP_NAME>	Specify local user group. Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests.
name <LOCAL_USER_NAME>	Specify local user. Local user object name. Example: <i>user1</i>

Example

included users all

Syntax

excluded users { administrator | app | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }

Mode

App Control Signature

Description

Set excluded users/groups.

Options

administrator	Built-in administrator.
app	Use app setting.
group <LOCAL_USER_GROUP_NAME>	Specify local user group. Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests.
name <LOCAL_USER_NAME>	Specify local user. Local user object name. Example: <i>user1</i>

Example

excluded users guests

Syntax

included ip { all | app | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

App Control Signature

Description

Set included IP address range.

Options

all	All.
app	Use app setting.
group <ADDR_GROUP_NAME>	Address object group Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

included ip range 10.10.10.1 10.10.10.10

Syntax

excluded ip { app | group <ADDR_GROUP_NAME> | host <ADDR_HOST> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> }

Mode

App Control Signature

Description

Set excluded IP address range.

Options

app	Use app setting.
group	Address object group
<ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
excluded ip range 10.10.10.1 10.10.10.10
```

Syntax

```
no excluded { ip | users }
```

Mode

App Control Signature

Description

Disable exclude users/groups or IP addresses.

Options

ip Disable exclude IP addresses.

users Disable exclude users/groups.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | app | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

App Control Signature

Description

Set app control signature schedule.

Options

<i>always-on</i>	Always on.
<i>app</i>	Use app setting.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule always-on

Syntax

log-redundancy { app | filter <UINT16> }

Mode

App Control Signature

Description

Set app control signature log redundancy filter.

Options

<i>app</i>	Use app setting.
<i>filter</i>	Set log redundancy filter in seconds.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

App Control Signature

Description

Clear app control signature log redundancy filter.

Options

<i>filter</i>	Set log redundancy filter in seconds.

Example

no log-redundancy filter

Syntax

rb1

Mode

Config

Description

Enter real-time blacklist configuration mode.

Example

rb1

Syntax

enable

Mode

RBL

Description

Enable real-time blacklist blocking.

Example

enable

Syntax

no enable

Mode

RBL

Description

Disable real-time blacklist blocking.

Example

no enable

Syntax

dns { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }

Mode

RBL

Description

Set whether RBL DNS is inherited from WAN Zone or set manually with the associated DNS server IP addresses.

Options

<i>inherit</i>	Inherit DNS servers.
<i>static</i>	Set static DNS server

<i>primary</i>	Specify primary DNS server IP address.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>secondary</i>	Specify secondary DNS server IP address.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>tertiary</i>	Specify tertiary DNS server IP address.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
dns primary 192.168.168.165
```

Syntax

```
no dns static { primary | secondary | tertiary }
```

Mode

RBL

Description

Manually clear DNS server IP address.

Options

<i>static</i>	Static DNS server
<i>primary</i>	Clear primary DNS server IP address.
<i>secondary</i>	Clear secondary DNS server IP address.
<i>tertiary</i>	Clear tertiary DNS server IP address.

Example

```
no dns primary
```

Syntax

```
service { domain <RBL_SERVICE_NAME> | enable <RBL_SERVICE_NAME> }
```

Mode

RBL

Description

Enable/add/edit real-time blacklist service.

Options

<i>domain</i>	real-time blacklist service name.
<i><RBL_SERVICE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>enable</i>	Enable specified parameter.
<i><RBL_SERVICE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
service domain avidspamsender.local
```

Syntax

```
no service { domain <RBL_SERVICE_NAME> | enable <RBL_SERVICE_NAME> }
```

Mode

RBL

Description

Delete real-time blacklist service.

Options

domain	Real-Time blacklist service bame.
<RBL_SERVICE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
enable	Enable specified parameter.
<RBL_SERVICE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
no service enable xxx.org
```

Syntax

```
no services
```

Mode

RBL

Description

Delete all RBL services.

Example

```
no services
```

Syntax

```
clear statistics [ service <RBL_SERVICE_NAME> ]
```

Mode

RBL

Description

Clear all or specified RBL service statistics.

Options

service	RBL service name.
<RBL_SERVICE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
clear statistics  
clear statistics service "dnsbl.sorbs.net"
```

Syntax

```
blacklist { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <RBL_ADDR_NAME> | range <ADDR_BEGIN> <ADDR_END> }
```

Mode

RBL

Description

Add SMTP server to blacklist.

Options

<i>fqdn</i> <ADDR_FQDN>	SMTP server Full Qualified Domain Name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i> <ADDR_HOST>	SMTP server host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <RBL_ADDR_NAME>	SMTP server named host address object. Address object name. Example: <i>Web Server</i>
<i>range</i> <ADDR_BEGIN>	SMTP server Range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
blacklist host 168.226.49.15
```

Syntax

```
no blacklist { fqdn <RBL_ADDR_FQDN> | host <RBL_ADDR_HOST> | name <RBL_ADDR_NAME> | range <RBL_ADDR_BEGIN> <RBL_ADDR_END> }
```

Mode

RBL

Description

Remove SMTP server from blacklist.

Options

<i>fqdn</i> <RBL_ADDR_FQDN>	SMTP server Full Qualified Domain Name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i> <RBL_ADDR_HOST>	SMTP server host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i> <RBL_ADDR_NAME>	SMTP server named host address object. Address object name. Example: <i>Web Server</i>
<i>range</i> <RBL_ADDR_BEGIN>	SMTP server Range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<RBL_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.

Example: *IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n*

Example

no blacklist host 168.226.49.15

Syntax

whitelist { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <RBL_ADDR_NAME> | range <ADDR_BEGIN> <ADDR_END> }

Mode

RBL

Description

Add SMTP server to whitelist.

Options

<i>fqdn</i>	SMTP server Full Qualified Domain Name.
<i><ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	SMTP server host address.
<i><ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	SMTP server named host address object.
<i><RBL_ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>
<i>range</i>	SMTP server Range.
<i><ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i><ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

whitelist host 168.226.49.15

Syntax

no whitelist { fqdn <RBL_ADDR_FQDN> | host <RBL_ADDR_HOST> | name <RBL_ADDR_NAME> | range <RBL_ADDR_BEGIN> <RBL_ADDR_END> }

Mode

RBL

Description

Remove SMTP server from whitelist.

Options

<i>fqdn</i>	SMTP server Full Qualified Domain Name.
<i><RBL_ADDR_FQDN></i>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i>	SMTP server host address.
<i><RBL_ADDR_HOST></i>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

<i>name</i>	SMTP server named host address object.
<i><RBL_ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>
<i>range</i>	SMTP server Range.
<i><RBL_ADDR_BEGIN></i>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i><RBL_ADDR_END></i>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>

Example

```
no whitelist host 168.226.49.15
```

Syntax

```
enable
```

Mode

RBL Service

Description

Enable real-time blacklist domain.

Example

```
enable
```

Syntax

```
no enable
```

Mode

RBL Service

Description

Disable real-time blacklist domain.

Example

```
no enable
```

Syntax

```
domain <RBL_SERVICE_NAME>
```

Mode

RBL Service

Description

Set real-time blacklist service domain bame.

Options

<i><RBL_SERVICE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
domain avidspamsender.local
```

Syntax

```
blocked-responses [ open-relay ] [ dialup-spam-source ] [ spam-source ] [ smart-host ] [ spamware-site ] [ bad-list-server ] [ insecure-script ] [ open-proxy-server ] [ policy-block-list-isp ] [ policy-block-list-domain ] [ block-all ]
```

Mode

RBL Service

Description

Enable specified RBL Blocked Responses.

Options

<i>open-relay</i>	127.0.0.2 - Open Relay.
<i>dialup-spam-source</i>	127.0.0.3 - Dialup Spam Source.
<i>spam-source</i>	127.0.0.4 - Spam Source.
<i>smart-host</i>	127.0.0.5 - Smart Host.
<i>spamware-site</i>	127.0.0.6 - Spamware Site.
<i>bad-list-server</i>	127.0.0.7 - Bad List Server.
<i>insecure-script</i>	127.0.0.8 - Insecure Script.
<i>open-proxy-server</i>	127.0.0.9 - Open Proxy Server.
<i>policy-block-list-isp</i>	127.0.0.10 - Policy Block List ISP.
<i>policy-block-list-domain</i>	127.0.0.11 - Policy Block List Domain Owner.
<i>block-all</i>	Block all responses.

Example

```
blocked-responses open-relay spamware-site
```

Syntax

```
no blocked-responses [ open-relay ] [ dialup-spam-source ] [ spam-source ] [ smart-host ] [ spamware-site ] [ bad-list-server ] [ insecure-script ] [ open-proxy-server ] [ policy-block-list-isp ] [ policy-block-list-domain ] [ block-all ]
```

Mode

RBL Service

Description

Disable specified RBL Blocked Responses.

Options

<i>open-relay</i>	127.0.0.2 - Open Relay.
<i>dialup-spam-source</i>	127.0.0.3 - Dialup Spam Source.
<i>spam-source</i>	127.0.0.4 - Spam Source.
<i>smart-host</i>	127.0.0.5 - Smart Host.
<i>spamware-site</i>	127.0.0.6 - Spamware Site.
<i>bad-list-server</i>	127.0.0.7 - Bad List Server.
<i>insecure-script</i>	127.0.0.8 - Insecure Script.
<i>open-proxy-server</i>	127.0.0.9 - Open Proxy Server.
<i>policy-block-list-isp</i>	127.0.0.10 - Policy Block List ISP.
<i>policy-block-list-domain</i>	127.0.0.11 - Policy Block List Domain Owner.
<i>block-all</i>	Block all responses.

Example

```
no blocked-responses open-relay spamware-site
```

Syntax

```
dpi-ssl { client | server }
```

Mode

Config

Description

Enter DPI-SSL configuration mode.

Options

- client** Enter client DPI-SSL configuration mode.
- server** Enter server DPI-SSL configuration mode.

Example

```
dpi-ssl server
dpi-ssl client
```

Syntax

```
export dpi-ssl-client certificate { default | default-2048-bit } { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

- Top Level
- Config
- Client DPI-SSL

Description

Export DPI-SSL client certificate to file.

Options

- default** Default SonicWall DPI-SSL 1024 bit CA certificate.
- default-2048-bit** Default SonicWall DPI-SSL 2048 bit CA certificate.
- api** Export using the api.
- ftp** Export using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\\\', '\\' -> '\\\\\\\\'.
Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/
- scp** Export using the SCP protocol.
<SCP_URL> SCP URL in the form: userName@serverip:/fileDirectory.
Example: userTest@10.10.10.10:/home/userTest/
- port** SCP server port
<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: 80

Example

```
export dpi-ssl-client certificate default ftp ftp://user:password@servername/dpi-ssl-2048-sha2.der
export dpi-ssl-client certificate default scp user@server:/home/user/dpi-ssl-2048-sha2.der
export dpi-ssl-client certificate default scp user@server:/home/user/
```

Syntax

```
import exclusions { api | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Client DPI-SSL

Description

Update default exclusions manually.

Options

api	Import using the api.
ftp	Import using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname\n Escape character: '.' -> '\\.', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port	SCP server port
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
import exclusions ftp ftp://user:password@servername/exclusions-tmp
import exclusions scp user@server:/home/user/exclusions-tmp
```

Syntax

enable

Mode

Client DPI-SSL

Description

Enable SSL client inspection.

Example

enable

Syntax

no enable

Mode

Client DPI-SSL

Description

Disable SSL client inspection.

Example

no enable

Syntax

intrusion-prevention

Mode

Client DPI-SSL

Description

Enable intrusion prevention for client DPI-SSL.

Example

intrusion-prevention

Syntax

no intrusion-prevention

Mode

Client DPI-SSL

Description

Disable intrusion prevention for client DPI-SSL.

Example

no intrusion-prevention

Syntax

gateway { anti-spyware | anti-virus }

Mode

Client DPI-SSL

Description

Enable gateway anti-virus or anti-spyware for client DPI-SSL.

Options

anti-spyware Enable gateway anti-spyware for client DPI-SSL.

anti-virus Enable gateway anti-virus for client DPI-SSL.

Example

gateway anti-virus

Syntax

no gateway { anti-spyware | anti-virus }

Mode

Client DPI-SSL

Description

Disable gateway anti-virus or anti-spyware for client DPI-SSL.

Options

anti-spyware Disable gateway anti-spyware for client DPI-SSL.

anti-virus Disable gateway anti-virus for client DPI-SSL.

Example

no gateway anti-virus

Syntax

application-firewall

Mode

Client DPI-SSL

Description

Enable application firewall for client DPI-SSL.

Example

```
application-firewall
```

Syntax

```
no application-firewall
```

Mode

Client DPI-SSL

Description

Disable application firewall for client DPI-SSL.

Example

```
no application-firewall
```

Syntax

```
content-filter
```

Mode

Client DPI-SSL

Description

Enable content filter for client DPI-SSL.

Example

```
content-filter
```

Syntax

```
no content-filter
```

Mode

Client DPI-SSL

Description

Disable content filter for client DPI-SSL.

Example

```
no content-filter
```

Syntax

```
authenticate-server-for-decrypted-connections
```

Mode

Client DPI-SSL

Description

Enable always authenticate server for decrypted connections for client DPI-SSL.

Example

```
authenticate-server-for-decrypte
```

Syntax

```
no authenticate-server-for-decrypte
```

Mode

Client DPI-SSL

Description

Disable always authenticate server for decrypted connections for client DPI-SSL.

Example

```
no authenticate-server-for-decrypte
```

Syntax

```
expired-ca
```

Mode

Client DPI-SSL

Description

Enable allow expired CA.

Example

```
expired-ca
```

Syntax

```
no expired-ca
```

Mode

Client DPI-SSL

Description

Disable allow expired CA.

Example

```
no expired-ca
```

Syntax

```
deployment-server-domains
```

Mode

Client DPI-SSL

Description

Enable deployment wherein the firewall sees a single server IP for different server domains, ex: proxy setup.

Example

```
deployment-server-domains
```

Syntax

```
no deployment-server-domains
```

Mode

Client DPI-SSL

Description

Disable deployment wherein the firewall sees a single server IP for different server domains, ex: proxy setup.

Example

```
no deployment-server-domains
```

Syntax

```
bypass-decryption
```

Mode

Client DPI-SSL

Description

Enable allow SSL without decryption (bypass) when connection limit exceeded.

Example

```
bypass-decryption
```

Syntax

```
no bypass-decryption
```

Mode

Client DPI-SSL

Description

Disable allow SSL without decryption (bypass) when connection limit exceeded.

Example

```
no bypass-decryption
```

Syntax

```
audit-built-in-exclusion
```

Mode

Client DPI-SSL

Description

Enable audit new built-in exclusion domain names prior to being added for exclusion.

Example

```
audit-built-in-exclusion
```

Syntax

no audit-built-in-exclusion

Mode

Client DPI-SSL

Description

Disable audit new built-in exclusion domain names prior to being added for exclusion.

Example

no audit-built-in-exclusion

Syntax

authenticate-server

Mode

Client DPI-SSL

Description

Enable always authenticate server before applying exclusion policy.

Example

authenticate-server

Syntax

no authenticate-server

Mode

Client DPI-SSL

Description

Disable always authenticate server before applying exclusion policy.

Example

no authenticate-server

Syntax

open-failed-connections

Mode

Client DPI-SSL

Description

Open failed connections (that are not deemed a security threat).

Example

open-failed-connections

Syntax

no open-failed-connections

Mode

Client DPI-SSL

Description

Fail-open failed connections (that are not deemed a security threat).

Example

no open-failed-connections

Syntax

resigning-authority { certificate <CERT_NAME> | default [2048-bit | none-2048-bit] }

Mode

Client DPI-SSL

Description

Set the re-signing authority certificate.

Options

certificate	Specify DPI-SSL CA certificate.
<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
default	Default SonicWall DPI-SSL 1024 bit CA certificate.
2048-bit	Default SonicWall DPI-SSL 2048 bit CA certificate.
none-2048-bit	Default SonicWall DPI-SSL 1024 bit CA certificate.

Example

resigning-authority certificate "Corp CA Certificate"

Syntax

include address { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion address object or group.

Options

ipv6	IPv6 address object.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n

<ADDR_MASK>	Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
all	All addresses.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
include address name "DPI Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion address object or group.

Options

ipv6	IPv6 address object.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.

<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclude address name "DPI Exclusion Object"
```

Syntax

```
no exclude address
```

Mode

Client DPI-SSL

Description

Clear exclusion address objects or group for DPI-SSL client.

Example

```
no exclude address
```

Syntax

```
include service { all | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion service object or group.

Options

all	All services.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
include service name "DPI Inclusion Service"
```

Syntax

```
exclude service { group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion service object or group.

Options

group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
exclude service name "DPI Exclusion Service"
```

Syntax

```
no exclude service
```

Mode

Client DPI-SSL

Description

Clear exclusion service objects or group for DPI-SSL client.

Example

```
no exclude service
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL inclusion user object or group.

Options

administrator	Administrator.

<i>all</i>	All users.
<i>group</i>	Group object name.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guest users.
<i>name</i>	User object name.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

```
include user group "DPI User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Client DPI-SSL

Description

Set the DPI-SSL exclusion user object or group.

Options

<i>administrator</i>	Administrator.
<i>group</i>	Group object name.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guest users.
<i>name</i>	User object name.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

```
exclude user group "DPI User Group"
```

Syntax

```
no exclude user
```

Mode

Client DPI-SSL

Description

Clear exclusion user for DPI-SSL client.

Example

```
no exclude user
```

Syntax

```
clear connection-failures [ name <DPI_SSL_CLIENT_CONNECT_FAILURE_ENTRY_NAME> ]
```

Mode

Client DPI-SSL

Description

Clear DPI-SSL client connection failure entries.

Options

name	Clear a specific DPI-SSL client connection-failure entry.
<DPI_SSL_CLIENT_CONNECT_FAILURE_ENTRY_NAME>	Client connection failure entry name. Example: <i>update.software.cloud</i>

Example

```
clear connection-failures
```

Syntax

```
reject <DPI_SSL_CLIENT_COMMON_NAME>
```

Mode

Client DPI-SSL

Description

Reject DPI-SSL client built-in common name.

Options

<DPI_SSL_CLIENT_COMMON_NAME>	Client DPI-SSL common name. Example: <i>update.software.local</i>

Example

```
reject .livemeeting.com
```

Syntax

```
accept <DPI_SSL_CLIENT_COMMON_NAME>
```

Mode

Client DPI-SSL

Description

Accept DPI-SSL client built-in common names.

Options

<DPI_SSL_CLIENT_COMMON_NAME>	Client DPI-SSL common name. Example: <i>update.software.local</i>

Example

```
accept .livemeeting.com
```

Syntax

```
no common-name <DPI_SSL_CLIENT_COMMON_NAME> [ action { exclude [ { authenticate-server | disable-authenticate-server } ] | skip-authentication | skip-content-filter-exclusion } ]
```

Mode

Description

Delete a DPI-SSLcommon name.

Options

<DPI_SSL_CLIENT_COMMON_NAME>	Client DPI-SSL common name. Example: <i>update.software.local</i>
action	Set the action for client DPI-SSL common name.
exclude	Set action as exclude.
authenticate-server	Enable always authenticate server before applying exclusion policy
disable-authenticate-server	Disable always authenticate server before applying exclusion policy
skip-authentication	Set action as skip authentication.
skip-content-filter-exclusion	Set action as skip CFS category-based exclusion.

Example

```
no common-name update.software.local
```

Syntax

```
no common-names [ exclude | skip-authentication | skip-content-filter-exclusion ]
```

Mode

Client DPI-SSL

Description

Delete all DPI-SSL common names.

Options

exclude	Delete DPI-SSL exclusion common names.
skip-authentication	Delete DPI-SSL client skip authentication common names.
skip-content-filter-exclusion	Delete DPI-SSL client skip CFS category-based exclusion common names.

Example

```
no common-names
no common-names exclude
no common-names skip-content-filter-exclusion
no common-names skip-authentication
```

Syntax

```
common-name <WORD> action { exclude [ { authenticate-server | disable-authenticate-server } ] | skip-authentication | skip-content-filter-exclusion }
```

Mode

Client DPI-SSL

Description

Add client DPI-SSL common name.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\".

action	Example: <i>abc</i> Set the action for client DPI-SSL common name.
exclude	Set action as exclude.
authenticate-server	Enable always authenticate server before applying exclusion policy
disable-authenticate-server	Disable always authenticate server before applying exclusion policy
skip-authentication	Set action as skip authentication.
skip-content-filter-exclusion	Set action as skip CFS category-based exclusion.

Example

```
common-name .sonicwall.com action skip-authentication
```

Syntax

```
cfs-categories { category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL> | exclude | include }
```

Mode

Client DPI-SSL

Description

Set content filter categories inclusion/exclusion.

Options

category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL>	Set inclusion/exclusion categories Content filter category number and name with additional \"all\". Example: <i>all</i>
exclude	Enable exclude CFS categories.
include	Enable include CFS categories.

Example

```
cfs-categories category "1. Violence/Hate/Racism"
cfs-categories category all
cfs-categories include
cfs-categories exclude
```

Syntax

```
no cfs-categories category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL>
```

Mode

Client DPI-SSL

Description

Clear content filter categories inclusion/exclusion.

Options

category <CONTENT_FILTER_CATEGORY_ID_NAME_HAVING_ALL>	Clear inclusion/exclusion categories Content filter category number and name with additional \"all\". Example: <i>all</i>

Example

```
no cfs-categories category all
no cfs-categories category "1. Violence/Hate/Racism"
```

Syntax

exclude cfs-category-unavailable

Mode

Client DPI-SSL

Description

Enable exclude connection if content filter category is not available.

Example

exclude cfs-category-unavailable

Syntax

no exclude cfs-category-unavailable

Mode

Client DPI-SSL

Description

Disable exclude connection if content filter category is not available.

Example

no exclude cfs-category-unavailable

Syntax

enable

Mode

Server DPI-SSL

Description

Enable SSL server inspection.

Example

enable

Syntax

no enable

Mode

Server DPI-SSL

Description

Disable SSL server inspection.

Example

no enable

Syntax

```
intrusion-prevention
```

Mode

Server DPI-SSL

Description

Enable intrusion prevention for server DPI-SSL.

Example

```
intrusion-prevention
```

Syntax

```
no intrusion-prevention
```

Mode

Server DPI-SSL

Description

Disable intrusion prevention for server DPI-SSL.

Example

```
no intrusion-prevention
```

Syntax

```
gateway { anti-spyware | anti-virus }
```

Mode

Server DPI-SSL

Description

Enable gateway anti-virus or anti-spyware for server DPI-SSL.

Options

anti-spyware Enable gateway anti-spyware for server DPI-SSL.

anti-virus Enable gateway anti-virus for server DPI-SSL.

Example

```
gateway anti-virus
```

Syntax

```
no gateway { anti-spyware | anti-virus }
```

Mode

Server DPI-SSL

Description

Disable gateway anti-virus or anti-spyware for server DPI-SSL.

Options

anti-spyware Disable gateway anti-spyware for server DPI-SSL.

anti-virus Disable gateway anti-virus for server DPI-SSL.

Example

no gateway anti-virus

Syntax

application-firewall

Mode

Server DPI-SSL

Description

Enable application firewall for server DPI-SSL.

Example

application-firewall

Syntax

no application-firewall

Mode

Server DPI-SSL

Description

Disable application firewall for server DPI-SSL.

Example

no application-firewall

Syntax

include address { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | all | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }

Mode

Server DPI-SSL

Description

Set the DPI-SSL inclusion address object or group.

Options

<i>ipv6</i>	IPv6 address object.
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>network</i> <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>

<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
all	All addresses.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
include address name "DPI Inclusion Object"
```

Syntax

```
exclude address { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL exclusion address object or group.

Options

ipv6	IPv6 address object.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com.

	Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

```
exclude address name "DPI Exclusion Object"
```

Syntax

```
include user { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL inclusion user object or group.

Options

administrator	Administrator.
all	All users.
group	Group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guest users.
name	User object name.
<LOCAL_USER_NAME>	Local user object name. Example: <i>user1</i>

Example

```
include user group "DPI User Group"
```

Syntax

```
exclude user { administrator | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> }
```

Mode

Server DPI-SSL

Description

Set the DPI-SSL exclusion user object or group.

Options

administrator	Administrator.
group	Group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name.

	Example: <i>Limited Administrators</i>
guests	Guest users.
name	User object name.
<LOCAL_USER_NAME>	Local user object name. Example: <i>user1</i>

Example

```
exclude user group "DPI User Group"
```

Syntax

```
no exclude { address | user }
```

Mode

Server DPI-SSL

Description

Clear exclusion for DPI-SSL server.

Options

address	Clear exclusion address object or group for DPI-SSL server.
user	Clear exclusion user or group for DPI-SSL server.

Example

```
no exclude address
```

Syntax

```
ssl-server [ ipv6 ] { fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } certificate <CERT_NAME> [ cleartext ]
```

Mode

Server DPI-SSL

Description

Add a DPI-SSL SSL server.

Options

ipv6	IPv6 address object.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Address object MAC. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.

<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
certificate	Set the DPI-SSL SSL server certificate.
<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
cleartext	Enable clear text on the back end.

Example

```
ssl-server host 192.168.168.172 certificate "Corp SSL Server Certificate" cleartext
ssl-server name mySSLServerAo certificate "Corp SSL Server Certificate"
ssl-server group sslServerGroup certificate "Corp SSL Server Certificate"
```

Syntax

```
no ssl-server { group <ADDR_GROUP_NAME_MIXED> | name <DPI_SSL_SSL_SERVER_NAME> } [ certificate <CERT_NAME> [ cleartext ] ]
```

Mode

Server DPI-SSL

Description

Delete a DPI-SSL SSL server.

Options

group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Address object name.
<DPI_SSL_SSL_SERVER_NAME>	SSL server name. Example: <i>DPI-SSL Server Name</i>
certificate	Set the DPI-SSL SSL server certificate.
<CERT_NAME>	Certificate name. Example: <i>my_cert</i>
cleartext	Enable clear text on the back end.

Example

```
no ssl-server name mySSLServerAo certificate "Corp SSL Server Certificate" cleartext
no ssl-server group sslServerGroup certificate "Corp SSL Server Certificate" noneclear
```

Syntax

```
no ssl-servers
```

Mode

Server DPI-SSL

Description

Delete all DPI-SSL SSL servers.

Example

```
no ssl-servers
```

Syntax

```
geo-ip
```

Mode

Config

Description

Enter Geo-IP configuration mode.

Example

```
geo-ip
```

Syntax

```
custom-list
```

Mode

Geo-IP

Description

Enter custom list configuration mode.

Example

```
custom-list
```

Syntax

```
enable
```

Mode

Custom List

Description

Enable Geo-IP custom list.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Custom List

Description

Disable Geo-IP custom list.

Example

```
no enable
```

Syntax

override-countries

Mode

Custom List

Description

Override firewall countries by custom list.

Example

override-countries

Syntax

no override-countries

Mode

Custom List

Description

Disable override firewall countries by custom list.

Example

no override-countries

Syntax

address { group <ADDR_CUSTOM_HNR_GROUP_NAME_MIXED> | name <ADDR_CUSTOM_HNR_NAME_MIXED> }

Mode

Custom List

Description

Set Geo-IP custom list IP address and enter address configuration mode.

Options

group	Set address group.
<ADDR_CUSTOM_HNR_GROUP_NAME_MIXED>	Host/network/range custom group address object name. Example: <i>Sales Group</i>
name	Set address object name.
<ADDR_CUSTOM_HNR_NAME_MIXED>	Host/network/range address object name. Example: <i>Web Server</i>

Example

address name "X5 Subnet"
address group "WLAN Subnets"

Syntax

no address { group <GEO_IP_ADDR_GROUP> | name <GEO_IP_ADDR_NAME> }

Mode

Custom List

Description

Delete a Geo-IP custom list IP address object.

Options

<i>group</i>	Address object group.
<i><GEO_IP_ADDR_GROUP></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>name</i>	Address object name.
<i><GEO_IP_ADDR_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
no address name "X5 Subnet"  
no address group "WLAN Subnets"
```

Syntax

```
no addresses
```

Mode

Custom List

Description

Delete all address objects from Geo-IP custom list.

Example

```
no addresses
```

Syntax

```
country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo IP Custom Country Entry

Description

Set the country.

Options

<i><GEO_IP_BLOCKED_COUNTRY></i>	Geo-IP blocked country name. Example: <i>Angola</i>

Example

```
country Antartica
```

Syntax

```
comment <WORD>
```

Mode

Geo IP Custom Country Entry

Description

Set the comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "USServer".
```

Syntax

```
no comment
```

Mode

Geo IP Custom Country Entry

Description

Clear the comment.

Example

```
no comment
```

Syntax

```
block connections [ all | firewall-rule-based ]
```

Mode

Geo-IP

Description

Set block connection method for Geo-IP.

Options

all All connections.

firewall-rule-based Firewall rule based connections.

Example

```
block connections firewall-rule-based
block connections all
block connections
```

Syntax

```
no block connections
```

Mode

Geo-IP

Description

Disable blocking connections to/from configured country list.

Example

```
no block connections
```

Syntax

```
block database-not-downloaded
```

Mode

Geo-IP

Description

Enable blocking all connections to public IPs if Geo-IP database is not downloaded.

Example

```
block database-not-downloaded
```

Syntax

```
no block database-not-downloaded
```

Mode

Geo-IP

Description

Disable blocking all connections to public IPs if Geo-IP database is not downloaded.

Example

```
no block database-not-downloaded
```

Syntax

```
logging
```

Mode

Geo-IP

Description

Enable Geo-IP filter logging.

Example

```
logging
```

Syntax

```
no logging
```

Mode

Geo-IP

Description

Disable Geo-IP filter logging.

Example

```
no logging
```

Syntax

```
block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo-IP

Description

Enable the country in the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
block country Antartica
```

Syntax

```
no block country <GEO_IP_BLOCKED_COUNTRY>
```

Mode

Geo-IP

Description

Disable the country in the configured country list.

Options

<GEO_IP_BLOCKED_COUNTRY> Geo-IP blocked country name.
Example: *Angola*

Example

```
no block country Canada
```

Syntax

```
block countries [ unknown ]
```

Mode

Geo-IP

Description

Set block countries for Geo-IP.

Options

unknown Enable block all unknown countries.

Example

```
block countries  
block countries unknown
```

Syntax

```
no block countries [ unknown ]
```

Mode

Geo-IP

Description

Set block countries for Geo-IP.

Options

unknown Disable block all unknown countries.

Example

no block countries
no block countries unknown

Syntax

no exclude

Mode

Geo-IP

Description

Clear Geo-IP exclusion objects.

Example

no exclude

Syntax

exclude { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> }

Mode

Geo-IP

Description

Set Geo-IP exclusion object.

Options

ipv6	IPv6
host <ADDR_HOST>	Geo-IP exclusion host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Geo-IP exclusion network IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Geo-IP exclusion range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
group <ADDR_GROUP_NAME_MIXED>	Geo-IP exclusion named address group. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Geo-IP exclusion named address object. Address object name.

Example

```
exclude name "X5 Subnet"  
exclude group "WLAN Subnets"  
exclude host 192.168.168.168  
exclude network 192.168.168.1 255.255.255.0  
exclude range 192.168.168.10 192.168.168.100  
exclude ipv6 host fe80::1001  
exclude ipv6 network fe80::1 /64  
exclude ipv6 range fe80::1001 fe80::1010
```

Syntax

```
include block-details
```

Mode

Geo-IP

Description

Enable inclusion of Geo-IP block details.

Example

```
include block-details
```

Syntax

```
no include block-details
```

Mode

Geo-IP

Description

Disable inclusion of Geo-IP block details.

Example

```
no include block-details
```

Syntax

```
alert-text <WORD>
```

Mode

Geo-IP

Description

Set the Geo-IP alert text.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
alert-text "This site had been blocked by the network administrator."
```

Syntax

no alert-text

Mode

Geo-IP

Description

Clear the Geo-IP alert text.

Example

no alert-text

Syntax

```
logo-icon { data <GEO_IP_LOGO_ICON_DATA> | ftp <FTP_URL> | scp <SCP_URL> [ port <IPV4_PORT> ] }
```

Mode

Geo-IP

Description

Set/Upload the Botnet Base64 encoded logo icon.

Options

data <GEO_IP_LOGO_ICON_DATA>	Set the Geo-IP Base64 encoded logo icon with user input. Geo-IP logo icon data. Example: <i>data:image/gif;base64,GEOIP/BOTNETLOGOICONDATA</i>
ftp <FTP_URL>	Import using the FTP protocol. FTP URL in the form: <i>ftp://username:password@hostname/</i> Escape character: <i>'\'</i> -> <i>'\\'</i> , <i>'@'</i> -> <i>'\\@'</i> , <i>'/'</i> -> <i>'\\/'</i> , <i>'\'</i> -> <i>'\\\\'</i> . Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp <SCP_URL>	Export using the SCP protocol. SCP URL in the form: <i>username@serverip/fileDirectory</i> . Example: <i>userTest@10.10.10.10:/home/userTest/</i>
port <IPV4_PORT>	SCP port. Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
logo-icon data "data:image/gif;base64,base64 encoded text goes here"
```

Syntax

default blocked-page

Mode

Geo-IP

Description

Set the blocked page settings to default.

Example

default blocked-page

Syntax

botnet

Mode

Config

Description

Enter botnet filter configuration mode.

Example

```
botnet
```

Syntax

```
custom-list
```

Mode

Botnet

Description

Enter custom list configuration mode.

Example

```
custom-list
```

Syntax

```
dynamic-list
```

Mode

Botnet

Description

Enter dynamic list configuration mode.

Example

```
dynamic-list
```

Syntax

```
block connections { all | firewall-rule-based }
```

Mode

Botnet

Description

Enable blocking connections to/from botnet command and control centers.

Options

all All connections.

firewall-rule-based Firewall rule based connections.

Example

```
block connections firewall-rule-based
```

Syntax

no block connections

Mode

Botnet

Description

Disable blocking connections to/from botnet command and control centers.

Example

no block connections

Syntax

block database-not-downloaded

Mode

Botnet

Description

Enable blocking all connections to public IPs if botnet database is not downloaded.

Example

block database-not-downloaded

Syntax

no block database-not-downloaded

Mode

Botnet

Description

Disable blocking all connections to public IPs if botnet database is not downloaded.

Example

no block database-not-downloaded

Syntax

enable

Mode

Custom List

Description

Enable botnet custom list.

Example

enable

Syntax

no enable

Mode

Custom List

Description

Disable botnet custom list.

Example

no enable

Syntax

address { group <ADDR_GROUP_NAME> | name <ADDR_NAME> }

Mode

Custom List

Description

Set botnet custom list IP address and enter address configuration mode.

Options

<i>group</i>	Set address group.
<i><ADDR_GROUP_NAME></i>	Group address object name. Example: <i>Sales Group</i>
<i>name</i>	Set address object name.
<i><ADDR_NAME></i>	Address object name. Example: <i>Web Server</i>

Example

address name "X5 Subnet"
address group "WLAN Subnets"

Syntax

no address { group <BOTNET_ADDR_GROUP> | name <BOTNET_ADDR_NAME> }

Mode

Custom List

Description

Delete a botnet custom list IP address object.

Options

<i>group</i>	Group address object.
<i><BOTNET_ADDR_GROUP></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>name</i>	Name address object.
<i><BOTNET_ADDR_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

no address name "X5 Subnet"
no address group "WLAN Subnets"

Syntax

no addresses

Mode

Custom List

Description

Delete all address objects from botnet custom list.

Example

no addresses

Syntax

name <ADDR_NAME>

Mode

Custom List Botnet Entry

Description

Botnet custom list name.

Options

<ADDR_NAME> Address object name.
Example: *Web Server*

Example

name "X5 Subnet"

Syntax

group <ADDR_GROUP_NAME>

Mode

Custom List Botnet Entry

Description

Botnet custom list group.

Options

<ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

Example

group "WLAN Subnets"

Syntax

enable

Mode

Custom List Botnet Entry

Description

Enable custom list botnet.

Example

enable

Syntax

no enable

Mode

Custom List Botnet Entry

Description

Disable custom list botnet.

Example

no enable

Syntax

comment <WORD>

Mode

Custom List Botnet Entry

Description

Set comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment "Remote USServer"

Syntax

no comment

Mode

Custom List Botnet Entry

Description

Clear comment.

Example

no comment

Syntax

enable

Mode

Dynamic List

Description

Enable botnet dynamic list.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Dynamic List

Description

Disable botnet dynamic list.

Example

```
no enable
```

Syntax

```
botnet-flush
```

Mode

Top Level
Config
Dynamic List

Description

Flush the IPs downloaded from dynamic botnet servers.

Example

```
botnet-flush
```

Syntax

```
botnet-download
```

Mode

Top Level
Config
Dynamic List

Description

Download the IPs downloaded from dynamic botnet servers.

Example

```
botnet-download
```

Syntax

```
periodical-download
```

Mode

Dynamic List

Description

Enable botnet list download periodically.

Example

```
periodical-download
```

Syntax

```
no periodical-download
```

Mode

Dynamic List

Description

Disable botnet list download periodically.

Example

```
no periodical-download
```

Syntax

```
download-interval { 15minutes | 1hour | 24hours | 5minutes }
```

Mode

Dynamic List

Description

Set a download interval for the dynamic botnet list server.

Options

15minutes Set the download interval as 15 minutes.

1hour Set the download interval as 1 hour.

24hours Set the download interval as 24 hours.

5minutes Set the download interval as 5 minutes.

Example

```
download-interval 5minutes
```

Syntax

```
protocol { ftp | https }
```

Mode

Dynamic List

Description

Set botnet server protocol type.

Options

ftp FTP protocol.

https HTTPS protocol.

Example

protocol https

Syntax

ftp server-ip-address <IPv4_HOST>

Mode

Dynamic List

Description

Set server IP address.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

ftp server-ip-address 2.2.2.2

Syntax

no ftp server-ip-address

Mode

Dynamic List

Description

Clear server IP address.

Example

no ftp server-ip-address

Syntax

ftp login <WORD>

Mode

Dynamic List

Description

Set login ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ftp login admin

Syntax

no ftp login

Mode

Dynamic List

Description

Clear login ID.

Example

```
no ftp login
```

Syntax

```
ftp password <ENC_PASSWORD>
```

Mode

Dynamic List

Description

Set password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
ftp password mypassword
```

Syntax

```
no ftp password
```

Mode

Dynamic List

Description

Clear password.

Example

```
no ftp password
```

Syntax

```
https login <WORD>
```

Mode

Dynamic List

Description

Set login ID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
https login admin
```

Syntax

no https login

Mode

Dynamic List

Description

Clear login ID.

Example

no https login

Syntax

https password <ENC_PASSWORD>

Mode

Dynamic List

Description

Set password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

https password mypassword

Syntax

no https password

Mode

Dynamic List

Description

Clear password.

Example

no https password

Syntax

ftp directory-path <WORD>

Mode

Dynamic List

Description

Set server directory path.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp directory-path "server/botnet"
```

Syntax

```
no ftp directory-path
```

Mode

Dynamic List

Description

Clear server directory path.

Example

```
no ftp directory-path
```

Syntax

```
ftp file-name <WORD>
```

Mode

Dynamic List

Description

Set server file name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ftp file-name aaa
```

Syntax

```
no ftp file-name
```

Mode

Dynamic List

Description

Clear server file name.

Example

```
no ftp file-name
```

Syntax

```
https url-name <WORD>
```

Mode

Dynamic List

Description

Set server url name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
https url-name www.SonicWall.com
```

Syntax

```
no https url-name
```

Mode

Dynamic List

Description

Clear server url name.

Example

```
no https url-name
```

Syntax

```
logging
```

Mode

Botnet

Description

Enable botnet filter logging.

Example

```
logging
```

Syntax

```
no logging
```

Mode

Botnet

Description

Disable botnet filter logging.

Example

```
no logging
```

Syntax

```
exclude { group <ADDR_GROUP_NAME_MIXED> | name <ADDR_HNR_NAME_MIXED> }
```

Mode

Botnet

Description

Set botnet exclusion object.

Options

<i>group</i>	Botnet exclusion named address group.
<i><ADDR_GROUP_NAME_MIXED></i>	Group address object name. Example: <i>Sales Group</i>
<i>name</i>	Botnet exclusion named address object.
<i><ADDR_HNR_NAME_MIXED></i>	Host/network/range address object name. Example: <i>Web Server</i>

Example

```
exclude name "X5 Subnet"  
exclude group "WLAN Subnets"
```

Syntax

```
no exclude
```

Mode

Botnet

Description

Clear botnet exclusion objects.

Example

```
no exclude
```

Syntax

```
include block-details
```

Mode

Botnet

Description

Enable inclusion of botnet block details.

Example

```
include block-details
```

Syntax

```
no include block-details
```

Mode

Botnet

Description

Disable inclusion of botnet block details.

Example

no include block-details

Syntax

alert-text <WORD>

Mode

Botnet

Description

Set the botnet alert text.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

alert-text "This site had been blocked by the network administrator"

Syntax

no alert-text

Mode

Botnet

Description

Set the botnet alert text.

Example

no alert-text

Syntax

logo-icon { data <GEO_IP_LOGO_ICON_DATA> | ftp <FTP_URL> | scp <SCP_URL> }

Mode

Botnet

Description

Set/Upload the botnet Base64 encoded logo icon.

Options

data Set the botnet base64 encoded logo icon data.
<GEO_IP_LOGO_ICON_DATA> Geo-IP logo icon data.
Example: *data:image/gif;base64,GEOIP/BOTNETLOGOICONDATA*

ftp Set base64 encoded logo icon data using the FTP protocol.
<FTP_URL> FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\V', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*

scp Set base64 encoded logo icon data using the SCP protocol.
<SCP_URL> SCP URL in the form: userName@serverip:/fileDirectory.
Example: *userTest@10.10.10.10:/home/userTest/*

Example

logo-icon data "data:image/gif;base64,base64 encoded text goes here"

Syntax

default blocked-page

Mode

Botnet

Description

Set the blocked page settings to default.

Example

default blocked-page

Syntax

anti-spyware

Mode

Config

Description

Enter anti-spyware configuration mode.

Example

anti-spyware

Syntax

update-signatures

Mode

Anti-spyware

Description

Update signature database.

Example

update-signatures

Syntax

enable

Mode

Anti-spyware

Description

Enable anti-spyware.

Example

enable

Syntax

no enable

Mode

Anti-spyware

Description

Disable anti-spyware.

Example

no enable

Syntax

signature-group { high-danger [prevent-all] [detect-all] [log-redundancy <UINT32>] | low-danger [prevent-all] [detect-all] [log-redundancy <UINT32>] | medium-danger [prevent-all] [detect-all] [log-redundancy <UINT32>] }

Mode

Anti-spyware

Description

Set signature group detection and log redundancy.

Options

high-danger High danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

low-danger Low danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

medium-danger Medium danger attacks.
prevent-all Prevent all.
detect-all Detect all.
log-redundancy Set log redundancy in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

signature-group high-danger prevent-all log-redundancy 1

Syntax

no signature-group { high-danger [prevent-all] [detect-all] [log-redundancy] | low-danger [prevent-all] [detect-all] [log-redundancy] | medium-danger [prevent-all] [detect-all] [log-redundancy] }

Mode

Anti-spyware

Description

Clear signature group detection.

Options

<i>high-danger</i>	High danger attacks.
<i>prevent-all</i>	Prevent all.
<i>detect-all</i>	Detect all.
<i>log-redundancy</i>	Set log redundancy in seconds.
<i>low-danger</i>	Low danger attacks.
<i>prevent-all</i>	Prevent all.
<i>detect-all</i>	Detect all.
<i>log-redundancy</i>	Set log redundancy in seconds.
<i>medium-danger</i>	Medium danger attacks.
<i>prevent-all</i>	Prevent all.
<i>detect-all</i>	Detect all.
<i>log-redundancy</i>	Set log redundancy in seconds.

Example

```
no signature-group high-danger prevent-all
```

Syntax

```
reset
```

Mode

Anti-spyware

Description

Reset anti-spyware settings and policies to default.

Example

```
reset
```

Syntax

```
inspection inbound [ http ] [ ftp ] [ imap ] [ smtp ] [ pop3 ]
```

Mode

Anti-spyware

Description

Enable inbound inspection for the specified protocols.

Options

<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.

Example

```
inspection inbound http smtp
```

Syntax

```
no inspection inbound [ http ] [ ftp ] [ imap ] [ smtp ] [ pop3 ]
```

Mode

Anti-spyware

Description

Disable inbound inspection for the specified protocols.

Options

http HTTP.
ftp FTP.
imap IMAP.
smtp SMTP.
pop3 POP3.

Example

```
no inspection inbound http smtp
```

Syntax

```
inspection outbound
```

Mode

Anti-spyware

Description

Enable inspection of outbound spyware communication.

Example

```
inspection outbound
```

Syntax

```
no inspection outbound
```

Mode

Anti-spyware

Description

Disable inspection of outbound spyware communication.

Example

```
no inspection outbound
```

Syntax

```
smtp-responses
```

Mode

Anti-spyware

Description

Enable SMTP responses.

Example

```
smtp-responses
```

Syntax

```
no smtp-responses
```

Mode

Anti-spyware

Description

Disable SMTP responses.

Example

```
no smtp-responses
```

Syntax

```
http-clientless-notification
```

Mode

Anti-spyware

Description

Enable HTTP clientless notification alerts.

Example

```
http-clientless-notification
```

Syntax

```
no http-clientless-notification
```

Mode

Anti-spyware

Description

Disable HTTP clientless notification alerts.

Example

```
no http-clientless-notification
```

Syntax

```
message <WORD>
```

Mode

Anti-spyware

Description

Set HTTP clientless notification message to display when blocking.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
message "This request is blocked by the SonicWall Gateway Anti-Spyware Service."
```

Syntax

no message

Mode

Anti-spyware

Description

Clear the notification message when blocking.

Example

no message

Syntax

exclusion { address { object | range } | address-object { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } | entry <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> <ANTI_SPYWARE_EXCLUSION_END_IP> | list }

Mode

Anti-spyware

Description

Set anti-spyware exclusion list and enable.

Options

address	Set exclusion list method.
object	Set exclusion list with address object.
range	Set exclusion list entry.
address-object	Set exclusion list with address object.
ipv6	IPv6 address.
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
fqdn <ADDR_FQDN>	Address object FQDN. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group. Group address object name. Example: <i>Sales Group</i>
mac	Address object MAC.

<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
entry	Set exclusion list entry.
<ANTI_SPYWARE_EXCLUSION_BEGIN_IP>	The from IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>
<ANTI_SPYWARE_EXCLUSION_END_IP>	The end IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>
list	Enable anti-spyware exclusion list.

Example

```
exclusion list
exclusion address-object name "All Interface IP"
exclusion entry 10.10.10.10 10.10.10.100
```

Syntax

```
from <ANTI_SPYWARE_EXCLUSION_BEGIN_IP>
```

Mode

Anti Spyware Exclusion Entry

Description

Set Anti spyware exclusion list entry start ip.

Options

<ANTI_SPYWARE_EXCLUSION_BEGIN_IP>	The from IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>

Example

```
from 10.10.10.1
```

Syntax

```
to <ANTI_SPYWARE_EXCLUSION_END_IP>
```

Mode

Anti Spyware Exclusion Entry

Description

Set Anti spyware exclusion list entry end ip.

Options

<ANTI_SPYWARE_EXCLUSION_END_IP>	The end IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>

Example

```
to 10.10.10.1
```

Syntax

```
no exclusion list
```

Mode

Anti-spyware

Description

Disable anti-spyware exclusion list.

Example

no exclusion list

Syntax

no exclusion entry <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> <ANTI_SPYWARE_EXCLUSION_END_IP>

Mode

Anti-spyware

Description

Delete anti-spyware exclusion list entry.

Options

- <ANTI_SPYWARE_EXCLUSION_BEGIN_IP>* The from IP of anti-spyware exclusion range list.
Example: *192.168.168.168*
- <ANTI_SPYWARE_EXCLUSION_END_IP>* The end IP of anti-spyware exclusion range list.
Example: *192.168.168.168*

Example

no exclusion entry 10.10.10.1 10.10.10.10

Syntax

no exclusion entries

Mode

Anti-spyware

Description

Delete all anti-spyware exclusion list entries.

Example

no exclusion entries

Syntax

product { id <ANTI_SPYWARE_PRODUCT_ID> | name <ANTI_SPYWARE_PRODUCT_NAME> } [policy id <ANTI_SPYWARE_POLICY_ID>]

Mode

Anti-spyware

Description

Enter configuration mode for the specified anti-spyware product.

Options

- id* Product ID.
- <ANTI_SPYWARE_PRODUCT_ID>* The ID of anti-spyware product.
Example: *123*
- name* Anti-spyware product name.

<ANTI_SPYWARE_PRODUCT_NAME>	The name of anti-spyware product. Example: <i>abc</i>
policy	Configure the anti-spyware policy and enter its configure mode.
id	Anti-spyware policy ID.
<ANTI_SPYWARE_POLICY_ID>	The policy ID of the specified anti-spyware product. Example: <i>123</i>

Example

```
product name "123mania"  
product id 940  
product name "180solutions" policy id 837
```

Syntax

```
name <WORD>
```

Mode

Anti-spyware Product
Anti-spyware Policy

Description

Anti-spyware product name or policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name 123minia
```

Syntax

```
id <UINT32>
```

Mode

Anti-spyware Product
Anti-spyware Policy

Description

Anti-spyware product ID or policy ID.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
id 3364
```

Syntax

```
prevention [ enable | global ]
```

Mode

Anti-spyware Product

Description

Set prevention for anti-spyware product.

Options

enable Enable anti-spyware product prevention.

global Use global setting.

Example

```
prevention global
```

Syntax

```
no prevention
```

Mode

Anti-spyware Product

Description

Disable prevention for anti-spyware product.

Example

```
no prevention
```

Syntax

```
detection [ enable | global ]
```

Mode

Anti-spyware Product

Description

Set detection for anti-spyware product.

Options

enable Enable anti-spyware product detection.

global Use global setting.

Example

```
detection
```

Syntax

```
no detection
```

Mode

Anti-spyware Product

Description

Disable detection for anti-spyware product.

Example

```
no detection
```

Syntax

```
included { ip { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } | users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } }
```

Mode

Anti-spyware Product

Description

Set included users or IP address ranges.

Options

ip	Set included IP address ranges.
all	All IP address ranges.
group <ADDR_GROUP_NAME_MIXED>	Group of IP address ranges. Group address object name. Example: <i>Sales Group</i>
name <ADDR_NAME_MIXED>	Name of IP address range. Address object name. Example: <i>Web Server</i>
users	Set included users or groups.
administrator	Administrator.
all	All users and groups.
group <LOCAL_USER_GROUP_NAME>	Group of users. Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests users.
name <USER_NAME>	Name of users. User object name. Example: <i>user1</i>

Example

```
included users all
included users name user1
included ip all
included ip name ao1
```

Syntax

```
excluded { ip { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } | users { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } }
```

Mode

Anti-spyware Product

Description

Set excluded users/groups or IP address ranges.

Options

ip	Set excluded IP address ranges.
all	All IP address ranges.
group	Group of IP address ranges.

<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Name of IP address range.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
users	Set excluded users or groups.
administrator	Administrator.
all	All users and groups.
group	Group of users.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests users.
name	Name of users.
<USER_NAME>	User object name. Example: <i>user1</i>

Example

```
excluded users administrator
excluded ip name aol
```

Syntax

```
no excluded { ip | users }
```

Mode

Anti-spyware Product

Description

Set no excluded users or IP address.

Options

ip Set no excluded IP address.

users Set no excluded users.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

Anti-spyware Product

Description

Set anti-spyware product schedule.

Options

always-on Always on.

<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule always-on

Syntax

log-redundancy { filter <UINT16> | global }

Mode

Anti-spyware Product

Description

Set anti-spyware product log redundancy filter.

Options

<i>filter</i>	Set log redundancy filter in seconds.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>global</i>	Use global setting.

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

Anti-spyware Product

Description

Clear anti-spyware product log redundancy filter.

Options

<i>filter</i>	Clear log redundancy filter in seconds.

Example

no log-redundancy filter

Syntax

product <WORD>

Mode

Description

Anti-spyware policy's product name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

product 123mania

Syntax

danger-level { high | low | medium }

Mode

Anti-spyware Policy

Description

Anti-spyware policy's danger level.

Options

high Anti-spyware policy high danger level.

low Anti-spyware policy low danger level.

medium Anti-spyware policy medium danger level.

Example

danger-level medium

Syntax

prevention [enable | product]

Mode

Anti-spyware Policy

Description

Set prevention for anti-spyware policy.

Options

enable Enable anti-spyware policy prevention.

product Use product setting.

Example

prevention product

Syntax

no prevention

Mode

Anti-spyware Policy

Description

Disable prevention for anti-spyware policy.

Example

```
no prevention
```

Syntax

```
detection [ enable | product ]
```

Mode

Anti-spyware Policy

Description

Set detection for anti-spyware policy.

Options

enable Enable anti-spyware policy detection.

product Use product setting.

Example

```
detection product
```

Syntax

```
no detection
```

Mode

Anti-spyware Policy

Description

Disable detection for anti-spyware policy.

Example

```
no detection
```

Syntax

```
included { ip { { { { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } } | product } } | users { { { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } } | product } } }
```

Mode

Anti-spyware Policy

Description

Set included users or IP address ranges.

Options

ip Set included IP address ranges.

all	All IP address ranges.
group	Group of IP address ranges.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Name of IP address range.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
product	Set included IP address ranges as product setting.
users	Set included users or groups.
administrator	Administrator.
all	All users and groups.
group	Group of users.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guests users.
name	Name of users.
<USER_NAME>	User object name. Example: <i>user1</i>
product	Set included users as product setting.

Example

```
included users all
included users name user1
included ip all
included ip name ao1
```

Syntax

```
excluded { ip { { { { all | group <ADDR_GROUP_NAME_MIXED> | name <ADDR_NAME_MIXED> } } | product } } | users { { { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <USER_NAME> } } | product } } }
```

Mode

Anti-spyware Policy

Description

Set excluded users/groups or IP address ranges.

Options

ip	Set excluded IP address ranges.
all	All IP address ranges.
group	Group of IP address ranges.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
name	Name of IP address range.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>
product	Set excluded IP address as product setting.

<i>users</i>	Set excluded users or groups.
<i>administrator</i>	Administrator.
<i>all</i>	All users and groups.
<i>group</i>	Group of users.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guests users.
<i>name</i>	Name of users.
<i><USER_NAME></i>	User object name. Example: <i>user1</i>
<i>product</i>	Set excluded users as product setting.

Example

```
excluded users administrator
excluded ip name aol
```

Syntax

```
no excluded { ip | users }
```

Mode

Anti-spyware Policy

Description

Set no excluded users or IP address.

Options

ip Set no excluded IP address.

users Set no excluded users.

Example

```
no excluded users
no excluded ip
```

Syntax

```
schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> | product }
```

Mode

Anti-spyware Policy

Description

Set anti-spyware product schedule.

Options

always-on Always on.

days Schedule object days.

<SCHED_DAYS> Days of the week in the form: SU-M-T-W-TH-F-SA.
Example: *SU-M-TH-SA*

time Schedule object beginning/ending time.

<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>
product	Use product setting.

Example

schedule always-on

Syntax

log-redundancy { filter <UINT16> | product }

Mode

Anti-spyware Policy

Description

Set anti-spyware product log redundancy filter.

Options

filter	Set log redundancy filter in seconds.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
product	Use product setting.

Example

log-redundancy filter 45

Syntax

no log-redundancy filter

Mode

Anti-spyware Policy

Description

Clear anti-spyware product log redundancy filter.

Options

filter	Clear log redundancy filter in seconds.

Example

no log-redundancy filter

Syntax

show security-services [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show security services configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show security-services

Syntax

show dpi-ssh [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show DPI-SSH configuration.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show dpi-ssh

Syntax

show content-filter [action { name | uuid } <CONTENT_FILTER_ACTION_NAME> | actions | cfs [{ base | custom-category [{ base | category-entries | category-entry <CFS_CUSTOM_CATEGORY_DOMAIN> }] | policies [statistics] | policy { name | uuid } <CFS_POLICY_NAME> [statistics] }] | profile { name | uuid } <CONTENT_FILTER_PROFILE_NAME> | profiles | settings | uri-list-group { name | uuid } <CONTENT_FILTER_URI_LIST_GRP_NAME> | uri-list-groups | uri-list-object { name | uuid } <CONTENT_FILTER_URI_LIST_OBJ_NAME> | uri-list-objects | websense | websense-status] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show content filter configuration and status.

Options

- action*** Content filter action object.
- name*** Show a CFS Action object by name.
- uuid*** Show a CFS Action object by UUID.
- <CONTENT_FILTER_ACTION_NAME>*** Content filter action object name.
Example: *Market action*
- actions*** All content filter action objects.
- cfs*** CFS configuration.

base	CFS base configuration.
custom-category	CFS custom category configuration.
base	CFS custom category base configuration.
category-entries	All CFS custom category entris.
category-entry	CFS custom category entry.
<CFS_CUSTOM_CATEGORY_DOMAIN>	CFS custom category domain. Example: <i>google.com</i>
policies	All CFS policies.
statistics	CFS policies statistics.
policy	CFS policy.
name	Show a CFS policy by name.
uuid	Show a CFS policy by UUID.
<CFS_POLICY_NAME>	CFS policy name. Example: <i>Market policy</i>
statistics	CFS policy statistics.
profile	Content filter profile object.
name	Show a CFS Profile object by name.
uuid	Show a CFS Profile object by UUID.
<CONTENT_FILTER_PROFILE_NAME>	Content filter profile object name. Example: <i>Market profile</i>
profiles	All content filter profile objects.
settings	Content-Filter configuration including CFS and Websense.
uri-list-group	Content fitler URI list group.
name	Show a CFS URL group object by name.
uuid	Show a CFS URL group object by UUID.
<CONTENT_FILTER_URI_LIST_GRP_NAME>	Content filter URI list group name. Example: <i>White URI list group</i>
uri-list-groups	All content fitler URI list groups.
uri-list-object	Content fitler URI list object.
name	Show a CFS URL object by name.
uuid	Show a CFS URL object by UUID.
<CONTENT_FILTER_URI_LIST_OBJ_NAME>	Content filter URI list object name. Example: <i>White URI list object</i>
uri-list-objects	All content fitler URI list objects.
websense	Websense.
websense-status	Websense Status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show content-filter
```

Syntax

```
show endpoint-security [ policies | policy <ENDPOINT_SECURITY_POLICY_NAME> | profile <ENDPOINT_SECURITY_PROFILE_NAME> |
profiles | settings | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show client enforcement configuration and status.

Options

<i>policies</i>	All Endpoint Security policies.
<i>policy</i> <ENDPOINT_SECURITY_POLICY_NAME>	Endpoint Security policy. Endpoint security policy name. Example: <i>Market policy</i>
<i>profile</i> <ENDPOINT_SECURITY_PROFILE_NAME>	Endpoint Security profile object. Endpoint security profile object name. Example: <i>Market profile</i>
<i>profiles</i>	All Endpoint Security profile objects.
<i>settings</i>	Endpoint Security common configurations.
<i>status</i>	Endpoint Security services status.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show endpoint-security
```

Syntax

```
show anti-spam [ [ allow-list | base | reject-list ] [ { pending-config | with-pending-config } ] | statistics [ { capture |
general | probe | threats } ] | status [ { monitoring | service } ] ]
```

Mode

All Modes

Description

Show anti-spam configuration and status.

Options

<i>allow-list</i>	Show anti-spam allow client list.
<i>base</i>	Show anti-spam global configuration.
<i>reject-list</i>	Show anti-spam reject client list.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>statistics</i>	Show anti-spam statistics.
<i>capture</i>	Show anti-spam packets capture statistics.

general	Show anti-spam general statistics.
probe	Show anti-spam monitoring probe statistics.
threats	Show anti-spam threats statistics.
status	Show anti-spam status.
monitoring	Show anti-spam monitoring status.
service	Show anti-spam service status.

Example

```
show anti-spam
show anti-spam allow-list
show anti-spam reject-list
show anti-spam status
show anti-spam status monitoring
show anti-spam statistics probe
show anti-spam statistics
```

Syntax

```
show intrusion-prevention [ categories | category { id <IPS_CATEGORY_ID> | name <IPS_CATEGORY_NAME> } [ [ policies | policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } ] ] | exclusion-list [ { base | entries | entry <IPS_EXCLUSION_BEGIN_IPV4_HOST> <IPS_EXCLUSION_END_IPV4_HOST> } ] | global | policies | policy { id <IPS_POLICY_ID> | name <IPS_POLICY_NAME> } | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show intrusion prevention configuration.

Options

categories	Show intrusion prevention categories.
category	Show intrusion prevention category.
id <IPS_CATEGORY_ID>	Category ID. Category ID. Example: <i>1234</i>
name <IPS_CATEGORY_NAME>	Category name. Category name. Example: <i>ACTIVEX</i>
policies	Show all policies of the specified IPS product.
policy	Show policy of the IPS category.
id <IPS_POLICY_ID>	Show IPS policy by ID. Policy ID. Example: <i>1234</i>
name <IPS_POLICY_NAME>	Show IPS policy by name. Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i>
exclusion-list	Show intrusion prevention exclusion list.
base	Show intrusion prevention exclusion list base configuration.
entries	Show intrusion prevention exclusion entries.
entry	Show IPS exclusion list entry.

<IPS_EXCLUSION_BEGIN_IPV4_HOST>	IPS Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
<IPS_EXCLUSION_END_IPV4_HOST>	IPS Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
global	Show intrusion prevention global configuration.
policies	Show intrusion prevention policies.
policy	Show intrusion prevention policy.
id <IPS_POLICY_ID>	Show IPS policy by ID. Policy ID. Example: <i>1234</i>
name <IPS_POLICY_NAME>	Show IPS policy by name. Policy name. Example: <i>ActivePDF WebGrabber ActiveX Instantiation</i>
status	Show intrusion prevention status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show intrusion-prevention
```



Syntax

```
show gateway-antivirus [ base | cloud [ { base | exclusions } ] | exclusion-list [ { base | entries | entry
<GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST> } ] | signatures | status ] [ { pending-config | with-pending-
config } ]
```

Mode

All Modes

Description

Show Gateway Anti-Virus configuration.

Options

base	Show Gateway Anti-Virus base settings.
cloud	Show Gateway Anti-Virus cloud configuration.
base	Show Gateway Anti-Virus cloud base configuration.
exclusions	Show Gateway Anti-Virus cloud exclusions configuration.
exclusion-list	Show Gateway Anti-Virus exclusion list.
base	Show Gateway Anti-Virus exclusion list base configuration.
entries	Show Gateway Anti-Virus exclusion list entries.
entry <GAV_EXCLUSION_BEGIN_IPV4_HOST> <GAV_EXCLUSION_END_IPV4_HOST>	Show Gateway AV exclusion list entry. Gateway AV Exclusion List entry begin IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i> Gateway AV Exclusion List entry end IPv4 in the form: D.D.D.D. Example: <i>192.168.168.168</i>
signatures	Show Gateway Anti-Virus signatures.
status	Show Gateway Anti-Virus status.

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show gateway-antivirus
```

Syntax

```
show capture-atp [ base | http-exclusions | md5-exclusions | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show capture ATP configuration and status.

Options

<i>base</i>	Show capture ATP base settings.
<i>http-exclusions</i>	Show capture ATP HTTP host names exclusions list settings.
<i>md5-exclusions</i>	Show capture ATP MD5 exclusions list settings.
<i>status</i>	Show capture ATP status
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show capture-atp
```

Syntax

```
show match-objects [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all match objects.

Options

<i>status</i>	Show match objects status.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show match-objects
```

Syntax

```
show match-object <MATCH_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show a match object.

Options

<MATCH_OBJ_NAME>	Match object name. Example: <i>Match FTP</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show match-object "Match FTP"
```

Syntax

```
show action-objects [ bandwidth-usage | default | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all action objects.

Options

bandwidth-usage	Show bandwidth usage.
default	Show all default action objects.
status	Show action objects status.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show action-objects
```

Syntax

```
show action-object <ACTION_OBJ_NAME> [ bandwidth-usage ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show action object configuration.

Options

<ACTION_OBJ_NAME>	Action object name. Example: <i>HTTP Block Page</i>
bandwidth-usage	Show bandwidth usage.

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show action-object CorpMailMessage
```

Syntax

```
show email-objects [ status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all e-mail address objects.

Options

- status*** Show e-mail user objects status.
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show email-objects
```

Syntax

```
show email-object <EMAIL_OBJ_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show an e-mail address Object.

Options

- <EMAIL_OBJ_NAME>*** E-mail object name.
Example: *Marketing E-mail Object*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show email-object "Client E-mail Addresses"
```

Syntax

```
show app-rules [ [ [ policies | policy <APP_RULES_POLICY_NAME> [ statistics ] ] ] [ { pending-config | with-pending-config } ] | base | status ]
```

Mode

All Modes

Description

Show app rule configuration.

Options

<i>polices</i>	Show app rule policies.
<i>policy</i>	Show app rule policy configuration.
<i><APP_RULES_POLICY_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>statistics</i>	Show app rule policies statistics.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>base</i>	Show app rule base configuration.
<i>status</i>	Show app rule status.

Example

show app-rules

Syntax

```
show app-control [ application { { id <AC_APP_ID> | name <AC_APP_NAME> } } [ [ signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures ] ] | applications | base | categories | category { { id <AC_CATEGORY_ID> | name <AC_CATEGORY_NAME> } } [ [ application { { id <AC_APP_ID> | name <AC_APP_NAME> } } [ [ signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures ] ] | applications | signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures ] ] | exclusion-list | signature { { id <AC_SIG_ID> | name <AC_SIG_NAME> } } | signatures | status ] [ { custom | default } ] [ { pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show app control configuration.

Options

<i>application</i>	Show app control application.
<i>id</i>	Application ID.
<i><AC_APP_ID></i>	Application ID. Example: <i>123</i>
<i>name</i>	Application name.
<i><AC_APP_NAME></i>	Application name. Example: <i>APP-UPDATE</i>
<i>signature</i>	Show app control signature of the specified application.
<i>id</i>	Signature ID.
<i><AC_SIG_ID></i>	Signature ID. Example: <i>123</i>
<i>name</i>	Signature name.
<i><AC_SIG_NAME></i>	Signature name.
<i>signatures</i>	Show app control signatures of the specified application.
<i>applications</i>	Show app control applications.
<i>base</i>	Show app control base configuration.

categories	Show app control categories.
category	Show app control category.
id	Category ID.
<AC_CATEGORY_ID>	Category ID. Example: <i>123</i>
name	Category name.
<AC_CATEGORY_NAME>	Category name. Example: <i>APP-UPDATE</i>
application	Show app control application of the specified category.
id	Application ID.
<AC_APP_ID>	Application ID. Example: <i>123</i>
name	Application name.
<AC_APP_NAME>	Application name. Example: <i>APP-UPDATE</i>
signature	Show app control signature of the specified application.
id	Signature ID.
<AC_SIG_ID>	Signature ID. Example: <i>123</i>
name	Signature name.
<AC_SIG_NAME>	Signature name.
signatures	Show app control signatures of the specified application.
applications	Show app control applications of the specified category.
signature	Show app control signature of the specified application.
id	Signature ID.
<AC_SIG_ID>	Signature ID. Example: <i>123</i>
name	Signature name.
<AC_SIG_NAME>	Signature name.
signatures	Show app control signatures of the specified application.
exclusion-list	Show app control exclusion list.
signature	Show app control signature.
id	Signature ID.
<AC_SIG_ID>	Signature ID. Example: <i>123</i>
name	Signature name.
<AC_SIG_NAME>	Signature name.
signatures	Show app control signatures.
status	Show app control status.
custom	Show custom configuration.
default	Show system/factory default configuration.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show app-control
```

Syntax

```
show rbl [ base | blacklist | service <RBL_SERVICE_NAME> | services | statistics [ service <RBL_SERVICE_NAME> ] | whitelist ]
[ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Real-Time Blacklist configuration.

Options

base	Show Real-Time Blacklist base configuration.
blacklist	Show RBL blacklist.
service <RBL_SERVICE_NAME>	Show Real-Time Blacklist service. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
services	Show Real-Time Blacklist services.
statistics service <RBL_SERVICE_NAME>	Show Real-Time Blacklist service statistics. Show Real-Time Blacklist service statistics by name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
whitelist	Show RBL whitelist.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show rbl
```

Syntax

```
show dpi-ssl [ client [ { base | cfs-categories | common-name <DPI_SSL_CLIENT_COMMON_NAME> | common-names | connection-
failures [ name <DPI_SSL_CLIENT_CONNECT_FAILURE_ENTRY_NAME> ] | default-exclusions-status } ] | server [ base | ssl-server
<DPI_SSL_SSL_SERVER_NAME> | ssl-servers ] ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show DPI-SSL configuration and status.

Options

client	Show client DPI-SSL configuration.
base	Show client DPI-SSL base settings.
cfs-categories	Show client DPI-SSL CFS categories settings.
common-name	Show a specific client DPI-SSL common name exclusions/inclusions setting.

<DPI_SSL_CLIENT_COMMON_NAME>	Client DPI-SSL common name. Example: <i>update.software.local</i>
<i>common-names</i>	Show client DPI-SSL common name exclusions/inclusions settings.
<i>connection-failures</i>	Show client DPI-SSL connection failures list.
<i>name</i>	Show a specific client DPI-SSL connection failure entry.
<DPI_SSL_CLIENT_CONNECT_FAILURE_ENTRY_NAME>	Client connection failure entry name. Example: <i>update.software.cloud</i>
<i>default-exclusions-status</i>	Show client DPI-SSL default exclusion status detail.
<i>server</i>	Show server DPI-SSL configuration.
<i>base</i>	Show DPI-SSL server base settings.
<i>ssl-server</i>	Show an specific DPI-SSL server SSL server.
<DPI_SSL_SSL_SERVER_NAME>	SSL server name. Example: <i>DPI-SSL Server Name</i>
<i>ssl-servers</i>	Show DPI-SSL server SSL servers settings.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show dpi-ssl
show dpi-ssl client
show dpi-ssl server
show dpi-ssl client connection-failures
```

Syntax

```
show geo-ip [ address { group <GEO_IP_ADDR_GROUP> | name <GEO_IP_ADDR_NAME> } | addresses | base | cache-statistics |
countries | custom-countries-statistics | resolved-locations | status ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show Geo-IP configuration.

Options

<i>address</i>	Show Geo-IP address in the custom Geo-IP list configurations.
<i>group</i>	Address group
<GEO_IP_ADDR_GROUP>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>name</i>	Address object
<GEO_IP_ADDR_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>addresses</i>	Show Geo-IP addresses in the custom Geo-IP list configurations.
<i>base</i>	Show Geo-IP base configurations.
<i>cache-statistics</i>	Show Geo-IP cache statistics.
<i>countries</i>	Show Geo-IP countries configurations.
<i>custom-countries-statistics</i>	Show Geo-IP custom country statistics.
<i>resolved-locations</i>	Show Geo-IP resolved locations.

<i>status</i>	Show Geo-IP database status.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show geo-ip
show geo-ip status
show geo-ip cache-statistics
show geo-ip custom-countries-statistics
show geo-ip resolved-locations
```

Syntax

```
show botnet [ [ { pending-config | with-pending-config } ] | base | cache-statistics | custom-list-address { group <WORD> | name <WORD> } | custom-list-addresses | resolved-locations | status ]
```

Mode

All Modes

Description

Show Botnet configuration.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>base</i>	Show Botnet global configuration.
<i>cache-statistics</i>	Show Botnet cache statistics.
<i>custom-list-address</i>	Show a specified Botnet custom list address.
<i>group</i> <WORD>	Botnet a custom list address group specified by name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>name</i> <WORD>	Botnet a custom list address object specified by name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>custom-list-addresses</i>	Show Botnet custom list addresses.
<i>resolved-locations</i>	Show Botnet resolved locations.
<i>status</i>	Show Botnet database status.

Example

```
show botnet
show botnet status
show botnet cache-statistics
show botnet resolved-locations
```

Syntax

```
show anti-spyware [ [ exclusion-list [ { base | entries | entry <ANTI_SPYWARE_EXCLUSION_BEGIN_IP> <ANTI_SPYWARE_EXCLUSION_END_IP> } ] | global | policies | policy id <ANTI_SPYWARE_POLICY_ID> | product { id <ANTI_SPYWARE_PRODUCT_ID> | name <ANTI_SPYWARE_PRODUCT_NAME> } [ [ policies | policy id <ANTI_SPYWARE_POLICY_ID> ] ] | products ] [ { pending-config | with-pending-config } ] | status ]
```

Mode

All Modes

Description

Show anti-spyware configuration or status.

Options

exclusion-list	Show anti-spyware exclusion list.
base	Show anti-spyware exclusion list base configuration.
entries	Show anti-spyware exclusion entries.
entry	Set exclusion list entry.
<ANTI_SPYWARE_EXCLUSION_BEGIN_IP>	The from IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>
<ANTI_SPYWARE_EXCLUSION_END_IP>	The end IP of anti-spyware exclusion range list. Example: <i>192.168.168.168</i>
global	Show anti-spyware global configuration.
policies	Show all anti-spyware policies.
policy	Show anti-spyware policy.
id	Show anti-spyware policy by ID.
<ANTI_SPYWARE_POLICY_ID>	The policy ID of the specified anti-spyware product. Example: <i>123</i>
product	Show anti-spyware product.
id	Show anti-spyware product by id.
<ANTI_SPYWARE_PRODUCT_ID>	The ID of anti-spyware product. Example: <i>123</i>
name	Show anti-spyware product by name.
<ANTI_SPYWARE_PRODUCT_NAME>	The name of anti-spyware product. Example: <i>abc</i>
policies	Show all policies of the specified anti-spyware product.
policy	Show policy of the anti-spyware product.
id	Show anti-spyware policy by ID.
<ANTI_SPYWARE_POLICY_ID>	The policy ID of the specified anti-spyware product. Example: <i>123</i>
products	Show anti-spyware products.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
status	Show anti-spyware status.

Example

show anti-spyware

Syntax

```
vpn [ policy { [ ipv4 ] { { group-vpn <VPN_GROUP_POLICY_NAME> | provision-client <VPN_PROVISION_CLIENT_POLICY_NAME> |  
provision-server <VPN_PROVISION_SERVER_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface  
<VPN_TUNNEL_POLICY_NAME> } } | enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } } ]
```

Mode

Config

Description

Configure VPN.

Options

policy	Add, edit or enable a VPN policy.
ipv4	IPv4 vpn policy.
group-vpn <VPN_GROUP_POLICY_NAME>	Edit group VPN policy. Group VPN policy name. Example: <i>WAN GroupVPN</i>
provision-client <VPN_PROVISION_CLIENT_POLICY_NAME>	Add or edit SonicWALL auto provisioning client VPN policy. SonicWALL auto provisioning client VPN policy name. Example: <i>SonicWALL auto provision client Policy</i>
provision-server <VPN_PROVISION_SERVER_POLICY_NAME>	Add or edit SonicWALL auto provisioning server VPN policy. SonicWALL auto provisioning server VPN policy name. Example: <i>SonicWALL auto provision server Policy</i>
site-to-site <VPN_SITE_POLICY_NAME>	Add or edit site-to-site VPN policy. Site-to-site VPN policy name. Example: <i>Remote Office</i>
tunnel-interface <VPN_TUNNEL_POLICY_NAME>	Add or edit tunnel interface VPN policy. Tunnel interface VPN policy name. Example: <i>Remote Office</i>
enable <VPN_POLICY_NAME>	Enable a VPN policy. VPN policy name. Example: <i>Remote Office</i>
ipv6	IPv6 vpn policy.
site-to-site <VPN_SITE_POLICY_V6_NAME>	Add or edit IPv6 site-to-site VPN policy. IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i>

Example

```
vpn
vpn policy site-to-site "Remote Office"
vpn policy group-vpn "WAN GroupVPN"
vpn policy enable "Remote Office"
```

Syntax

```
no vpn policy { [ ipv4 ] { { provision-client <VPN_PROVISION_CLIENT_POLICY_NAME> | provision-server
<VPN_PROVISION_SERVER_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } |
enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

Config

Description

Delete or disable a VPN policy.

Options

ipv4	IPv4 vpn policy.
provision-client <VPN_PROVISION_CLIENT_POLICY_NAME>	Delete SonicWALL auto provisioning client VPN policy. SonicWALL auto provisioning client VPN policy name. Example: <i>SonicWALL auto provision client Policy</i>
provision-server	Delete SonicWALL auto provisioning server VPN policy.

<VPN_PROVISION_SERVER_POLICY_NAME>	SonicWALL auto provisioning server VPN policy name. Example: <i>SonicWALL auto provision server Policy</i>
site-to-site	Delete site-to-site VPN policy.
<VPN_SITE_POLICY_NAME>	Site-to-site VPN policy name. Example: <i>Remote Office</i>
tunnel-interface	Delete tunnel interface VPN policy.
<VPN_TUNNEL_POLICY_NAME>	Tunnel interface VPN policy name. Example: <i>Remote Office</i>
enable	Enable a VPN policy.
<VPN_POLICY_NAME>	VPN policy name. Example: <i>Remote Office</i>
ipv6	IPv6 vpn policy.
site-to-site	Delete IPv6 site-to-site VPN policy.
<VPN_SITE_POLICY_V6_NAME>	IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i>

Example

```
no vpn policy site-to-site "Remote Office"
no vpn policy enable "Remote Office"
```

Syntax

```
no vpn policies
```

Mode

Config

Description

Delete all VPN policies.

Example

```
no vpn policies
```

Syntax

```
no vpn policies-ipv4
```

Mode

Config

Description

Delete all IPv4 VPN policies.

Example

```
no vpn policies-ipv4
```

Syntax

```
no vpn policies-ipv6
```

Mode

Config

Description

Delete all IPv6 VPN policies.

Example

no vpn policies-ipv6

Syntax

renegotiate tunnel <UINT8> <IP_V4V6_HOST> <IP_V4V6_HOST> <UINT8> <IP_V4V6_HOST> <IP_V4V6_HOST> <WORD> <IP_V4V6_HOST> <UINT32> <UINT8> <UINT32>

Mode

VPN

Description

Renegotiate the specific VPN tunnel.

Options

- <UINT8> Integer in the form: D OR 0xHH.
Example: 123
- <IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
- <IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
- <UINT8> Integer in the form: D OR 0xHH.
Example: 123
- <IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
- <IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
- <IP_V4V6_HOST> IPv4: address in the form: D.D.D.D\nIPv6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652
- <UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123
- <UINT8> Integer in the form: D OR 0xHH.
Example: 123
- <UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

renegotiate tunnel 4 192.16.16.0 255.255.255.0 4 192.168.168.0 255.255.255.0 "scn4i4GkZfI=" 10.8.16.13 500 0 2348292256

Syntax

enable

Mode

VPN

Description

Enable VPN.

Example

enable

Syntax

no enable

Mode

VPN

Description

Disable VPN.

Example

```
no enable
```

Syntax

```
firewall-identifier <WORD>
```

Mode

VPN

Description

Configure unique firewall identifier.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
firewall-identifier CorpFirewall
```

Syntax

```
ike-dpd
```

Mode

VPN

Description

Enter IKE dead peer detection mode.

Example

```
ike-dpd
```

Syntax

```
enable
```

Mode

IKE Dead Peer Detection

Description

Enable IKE dead peer detection.

Example

```
enable-ike-dpd
```

Syntax

```
no enable
```

Mode

Description

Disable IKE dead peer detection.

Example

```
no enable
```

Syntax

```
interval <UINT8>
```

Mode

IKE Dead Peer Detection

Description

Configure dead peer detection interval.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interval 60
```

Syntax

```
trigger <UINT8>
```

Mode

IKE Dead Peer Detection

Description

Configure failure trigger level in number of heartbeats.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
trigger 3
```

Syntax

```
idle-dpd
```

Mode

IKE Dead Peer Detection

Description

Enable dead peer detection for idle VPN sessions.

Example

```
idle-dpd
```

Syntax

```
no idle-dpd
```

Mode

IKE Dead Peer Detection

Description

Disable dead peer detection for idle VPN sessions.

Example

```
no idle-dpd
```

Syntax

```
idle-dpd-interval <UINT16>
```

Mode

IKE Dead Peer Detection

Description

Enable dead peer detection for idle VPN sessions.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
idle-dpd interval 600
```

Syntax

```
frag-packets
```

Mode

VPN

Description

Enter frag packets mode.

Example

```
frag-packets
```

Syntax

```
enable
```

Mode

Fragmented Packet Handling

Description

Enable and configure fragmented packet handling for VPN.

Example

```
enable
```

Syntax

no enable

Mode

Fragmented Packet Handling

Description

Disable fragmented packet handling for VPN.

Example

no enable

Syntax

ignore-df-bit

Mode

Fragmented Packet Handling

Description

Ignore DF (don't fragment) bit.

Example

ignore-df-bit

Syntax

no ignore-df-bit

Mode

Fragmented Packet Handling

Description

Disable ignore DF (don't fragment) bit.

Example

no ignore-df-bit

Syntax

nat-traversal

Mode

VPN

Description

Enable NAT traversal.

Example

nat-traversal

Syntax

no nat-traversal

Mode

VPN

Description

Disable NAT traversal.

Example

```
no nat-traversal
```

Syntax

```
cleanup-tunnels
```

Mode

VPN

Description

Enable clean up active tunnels when peer gateway DNS name resolves to a different IP address.

Example

```
cleanup-tunnels
```

Syntax

```
no cleanup-tunnels
```

Mode

VPN

Description

Disable clean up active tunnels when peer gateway DNS name resolves to a different IP address.

Example

```
no cleanup-tunnels
```

Syntax

```
preserve-ike-port
```

Mode

VPN

Description

Enable preserve IKE port for pass through connections.

Example

```
preserve-ike-port
```

Syntax

```
no preserve-ike-port
```

Mode

VPN

Description

Disable preserve IKE port for pass through connections.

Example

```
no preserve-ike-port
```

Syntax

```
ocsp-checking
```

Mode

VPN

Description

Enable OCSP checking.

Example

```
ocsp-checking
```

Syntax

```
no ocsp-checking
```

Mode

VPN

Description

Disable OCSP checking.

Example

```
no ocsp-checking
```

Syntax

```
responder-url <WEB_URL>
```

Mode

VPN

Description

Configure OCSP responder URL.

Options

<WEB_URL> URL in the form: http://host/file.
Example: `http://www.example.com/products/`

Example

```
responder-url http://www.sonicwall.com/ocsp
```

Syntax

```
no responder-url
```

Mode

VPN

Description

Clear OSCP responder URL.

Example

```
no responder-url
```

Syntax

```
traps-on-change
```

Mode

VPN

Description

Enable VPN tunnel traps only when tunnel status changes.

Example

```
traps-on-change
```

Syntax

```
no traps-on-change
```

Mode

VPN

Description

Disable VPN tunnel traps only when tunnel status changes.

Example

```
no traps-on-change
```

Syntax

```
use-radius { mschap | mschapv2 }
```

Mode

VPN

Description

Enable use RADIUS in specified mode for XAUTH.

Options

mschap Use MSCHAP for RADIUS.

mschapv2 Use MSCHAPv2 for RADIUS.

Example

```
use-radius mschapv2
```

Syntax

```
no use-radius
```

Mode

VPN

Description

Disable use RADIUS for XAUTH.

Example

```
no use-radius
```

Syntax

```
dns server { inherit | static { primary <IPV4_HOST> | secondary <IPV4_HOST> | tertiary <IPV4_HOST> } }
```

Mode

VPN

Description

Manually set DNS settings or inherit DNS settings dynamically from the SonicWall's DNS settings.

Options

<i>inherit</i>	Inherit DNS servers.
<i>static</i>	Static DNS server.
<i>primary</i> <IPV4_HOST>	Specify primary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>secondary</i> <IPV4_HOST>	Specify secondary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>tertiary</i> <IPV4_HOST>	Specify ternary DNS server IP address. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
dns server static primary 192.168.168.165  
dns server inherit
```

Syntax

```
no dns server static { primary | secondary | tertiary }
```

Mode

VPN

Description

Manually clear DNS server IP address.

Options

<i>static</i>	Static DNS server.
<i>primary</i>	Primary DNS server IP address.
<i>secondary</i>	Secondary DNS server IP address.

tertiary Ternary DNS server IP address.

Example

```
no dns server primary
```

Syntax

```
wins { primary <IPV4_HOST> | secondary <IPV4_HOST> }
```

Mode

VPN

Description

Set the WINS server IP address.

Options

primary Primary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

secondary Secondary WINS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

VPN

Description

Manually clear WINS server IP address.

Options

primary Primary WINS server IP address.

secondary Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
ikev2
```

Mode

VPN

Description

Configure IKEv2.

Example

```
ikev2
```

Syntax

```
send-cookie
```

Mode

IKEv2

Description

Enable send IKEv2 cookie notify.

Example

```
send-cookie
```

Syntax

```
no send-cookie
```

Mode

IKEv2

Description

Disable send IKEv2 cookie notify.

Example

```
no send-cookie
```

Syntax

```
send-invalid-spi
```

Mode

IKEv2

Description

Enable send IKEv2 invalid spi notify.

Example

```
send-invalid-spi
```

Syntax

```
no send-invalid-spi
```

Mode

IKEv2

Description

Disable send IKEv2 invalid spi notify.

Example

```
no send-invalid-spi
```

Syntax

```
proposal dh-group { 1 | 14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 }
```

Mode

IKEv2

Description

Configure IKEv2 DH group.

Options

- 1** Group 1 modp768.
- 14** Group 14 modp2048.
- 19** Group 19 ECP random 256-bit.
- 2** Group 2 modp1024.
- 20** Group 20 ECP random 384-Bit.
- 21** Group 21 ECP random 521-Bit.
- 25** Group 25 ECP random 192-Bit.
- 26** Group 26 ECP random 224-Bit.
- 5** Group 5 modp1536.

Example

```
proposal dh-group 2
```

Syntax

```
proposal encryption { aes-128 | aes-192 | aes-256 | des | triple-des }
```

Mode

IKEv2

Description

Configure IKEv2 encryption algorithm.

Options

- aes-128** Advanced encryption standard (AES) - 128 bit.
- aes-192** Advanced encryption standard (AES) - 192 bit.
- aes-256** Advanced encryption standard (AES) - 256 bit.
- des** Data encryption standard (DES).
- triple-des** Triple data encryption standard (3DES).

Example

```
proposal encryption aes-128
```

Syntax

```
proposal authentication { md5 | sha-1 | sha-256 | sha-384 | sha-512 }
```

Mode

IKEv2

Description

Configure IKEv2 authentication hashing algorithm.

Options

- md5** Message-digest algorithm 5 (MD5).
- sha-1** Secure hash algorithm 1 (SHA-1).
- sha-256** Secure hash algorithm 256 (SHA-256).
- sha-384** Secure hash algorithm 384 (SHA-384).
- sha-512** Secure hash algorithm 512 (SHA-512).

Example

```
proposal authentication md5
```

Syntax

```
policy { [ ipv4 ] { { group-vpn <VPN_GROUP_POLICY_NAME> | provision-client <VPN_PROVISION_CLIENT_POLICY_NAME> | provision-server <VPN_PROVISION_SERVER_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } | enable <VPN_POLICY_NAME> } | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

VPN

Description

Add, edit or enable a VPN policy.

Options

- ipv4** IPv4 vpn policy.
- group-vpn** Edit group VPN policy.
<VPN_GROUP_POLICY_NAME> Group VPN policy name.
Example: *WAN GroupVPN*
- provision-client** Add or edit SonicWALL auto provisioning client VPN policy.
<VPN_PROVISION_CLIENT_POLICY_NAME> SonicWALL auto provisioning client VPN policy name.
Example: *SonicWALL auto provision client Policy*
- provision-server** Add or edit SonicWALL auto provisioning server VPN policy.
<VPN_PROVISION_SERVER_POLICY_NAME> SonicWALL auto provisioning server VPN policy name.
Example: *SonicWALL auto provision server Policy*
- site-to-site** Add or edit site-to-site VPN policy.
<VPN_SITE_POLICY_NAME> Site-to-site VPN policy name.
Example: *Remote Office*
- tunnel-interface** Add or edit tunnel interface VPN policy.
<VPN_TUNNEL_POLICY_NAME> Tunnel interface VPN policy name.
Example: *Remote Office*
- enable** Enable a VPN policy.
<VPN_POLICY_NAME> VPN policy name.
Example: *Remote Office*

ipv6	IPv6 vpn policy.
site-to-site	Delete IPv6 site-to-site VPN policy.
<VPN_SITE_POLICY_V6_NAME>	IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i>

Example

```
policy site-to-site "Remote Office"
policy group-vpn "WAN GroupVPN"
policy enable "Remote Office"
```

Syntax

```
no policy { [ ipv4 ] { { provision-client <VPN_PROVISION_CLIENT_POLICY_NAME> | provision-server
<VPN_PROVISION_SERVER_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } |
enable <VPN_POLICY_NAME> | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } }
```

Mode

VPN

Description

Delete or disable a VPN policy.

Options

ipv4	IPv4 vpn policy.
provision-client	Delete SonicWALL auto provisioning client VPN policy.
<VPN_PROVISION_CLIENT_POLICY_NAME>	SonicWALL auto provisioning client VPN policy name. Example: <i>SonicWALL auto provision client Policy</i>
provision-server	Delete SonicWALL auto provisioning server VPN policy.
<VPN_PROVISION_SERVER_POLICY_NAME>	SonicWALL auto provisioning server VPN policy name. Example: <i>SonicWALL auto provision server Policy</i>
site-to-site	Delete site-to-site VPN policy.
<VPN_SITE_POLICY_NAME>	Site-to-site VPN policy name. Example: <i>Remote Office</i>
tunnel-interface	Delete tunnel interface VPN policy.
<VPN_TUNNEL_POLICY_NAME>	Tunnel interface VPN policy name. Example: <i>Remote Office</i>
enable	Enable a VPN policy.
<VPN_POLICY_NAME>	VPN policy name. Example: <i>Remote Office</i>
ipv6	IPv6 vpn policy.
site-to-site	Delete IPv6 site-to-site VPN policy.
<VPN_SITE_POLICY_V6_NAME>	IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i>

Example

```
no policy site-to-site "Remote Office"
no policy enable "Remote Office"
```

Syntax

```
no policies [ ipv4 { { provision-client | provision-server | site-to-site | tunnel-interface } } | ipv6 site-to-site ]
```

Mode

VPN

Description

Delete all VPN policies.

Options

<i>ipv4</i>	IPv4 vpn policy.
<i>provision-client</i>	Delete SonicWALL auto provisioning client VPN policy.
<i>provision-server</i>	Delete SonicWALL auto provisioning server VPN policy.
<i>site-to-site</i>	Delete site-to-site VPN policy.
<i>tunnel-interface</i>	Delete tunnel interface VPN policy.
<i>ipv6</i>	IPv6 vpn policy.
<i>site-to-site</i>	Delete IPv6 site-to-site VPN policy.

Example

no policies

Syntax

name <VPN_POLICY_NAME>

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning client VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Configure policy name.

Options

<VPN_POLICY_NAME> VPN policy name.
Example: *Remote Office*

Example

name "Remote Office"

Syntax

name <VPN_SITE_POLICY_V6_NAME>

Mode

Site to Site VPN IPv6 Policy

Description

Configure policy name.

Options

<VPN_SITE_POLICY_V6_NAME> IPv6 Site-to-site VPN policy name.
Example: *Remote Office*

Example

name "Remote Office"

Syntax

enable

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning client VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Enable VPN policy.

Example

enable

Syntax

no enable

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning client VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Disable VPN policy.

Example

no enable

Syntax

gateway primary <WORD>

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning client VPN Policy

Description

Configure the IPsec gateway name or address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

gateway primary 10.10.10.1

Syntax

no gateway primary

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning client VPN Policy

Description

Clear the IPsec gateway name or address.

Example

```
no gateway primary
```

Syntax

```
gateway secondary <WORD>
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the IPsec gateway name or address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
gateway secondary 10.10.10.1
```

Syntax

```
no gateway secondary
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the IPsec gateway name or address.

Example

```
no gateway secondary
```

Syntax

```
auth-method { certificate | manual-key | shared-secret }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Configure VPN policy authentication method.

Options

certificate IKE using 3rd party certificates.

- manual-key** Manual key.
- shared-secret** IKE using pre-shared secret.

Example

```
auth-method shared-secret
```

Syntax

```
auth-method { certificate | shared-secret }
```

Mode

Group VPN

Description

Configure VPN policy authentication method.

Options

- certificate** IKE using 3rd party certificates.
- shared-secret** IKE using pre-shared secret.

Example

```
auth-method shared-secret
```

Syntax

```
export group-vpn <VPN_GROUP_POLICY_ENABLE_NAME> { rcf { network { group <VPN_ADDR_GROUP_NAME> | name <VPN_ADDR_NAME> } [ password <WORD> ] { ftp <FTP_URL> } } | spd ftp <FTP_URL> }
```

Mode

VPN
Config

Description

Export a group VPN client policy file to FTP server.

Options

- <VPN_GROUP_POLICY_ENABLE_NAME>** Group VPN policy name.
Example: *WAN GroupVPN*
- rcf** Rcf format is required for Global VPN Clients.
- network** Configure the client access network(s) you wish to export.
- group** Select the network to named address object group.
- <VPN_ADDR_GROUP_NAME>** Group address object name.
Example: *Sales Group*
- name** Select the network to named address object.
- <VPN_ADDR_NAME>** Host/network/range address object name.
Example: *Web Server*
- password** You may encrypt the exported file using a chosen password.
- <WORD>** Word in the form: WORD or "QUOTED STRING".
Example: *abc*
- ftp** Export using the FTP protocol.
- <FTP_URL>** FTP URL in the form: ftp://username:password@hostname/
Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'.
Example: *ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/*
- spd** Spd format is required for VPN Clients 8.x and earlier.

ftp	Export using the FTP protocol.
<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\@', '/' -> '\\/', '\\' -> '\\\\\\\\'. Example: ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/

Example

export group-vpn WAN\\ GroupVPN rcf network name LANSubnets ftp ftp://user:password@servername/WAN\\ GroupVPN.rcf

Syntax

auth-method { certificate | shared-secret }

Mode

SonicWALL auto provisioning client VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Configure VPN policy authentication method.

Options

- certificate** Certificates.
- shared-secret** Pre-shared secret.

Example

auth-method shared-secret

Syntax

ap-client-id <WORD>

Mode

Preshared Secret

Description

Set VPN AP client ID.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

ap-client-id xxxx

Syntax

no ap-client-id

Mode

Preshared Secret

Description

Clear VPN AP client ID.

Example

no ap-client-id

Syntax

use-default-key

Mode

Preshared Secret

Description

Enable use default provisioning key.

Example

use-default-key

Syntax

no use-default-key

Mode

Preshared Secret

Description

Disable use default provisioning key.

Example

no use-default-key

Syntax

shared-secret <ENC_PASSWORD>

Mode

Preshared Secret

Description

Configure the pre-shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

shared-secret mysecret

Syntax

no shared-secret

Mode

Preshared Secret

Description

Clear the pre-shared secret.

Example

no shared-secret

Syntax

shared-secret <ENC_PASSWORD>

Mode

IKE Preshared Secret

Description

Configure the pre-shared secret.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

shared-secret mysecret

Syntax

no shared-secret

Mode

IKE Preshared Secret

Description

Clear the pre-shared secret.

Example

no shared-secret

Syntax

ike-id local { domain-name <VPN_FQDN> | email-address <EMAIL> | firewall-id <WORD> | ipv4 <IPV4_HOST> | ipv6 <IPV6_HOST> | key-id <WORD> }

Mode

IKE Preshared Secret

Description

Configure local IKE authentication associated identifiers.

Options

domain-name Domain name identifier.
<VPN_FQDN> Domain name in the form: aaa.aa.
Example: *example.com*

email-address E-mail address identifier.
<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

firewall-id Firewall identifier.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

ipv4 IP address identifier.

<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
ipv6 <IPV6_HOST>	IPv6 address identifier. IPV6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
key-id <WORD>	Key ID identifier. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
ike-id local email-address user@domain.com
```

Syntax

```
no ike-id local { domain-name | email-address | firewall-id | ipv4 | ipv6 | key-id }
```

Mode

IKE Preshared Secret

Description

Clear local IKE authentication associated identifiers.

Options

domain-name	Clear domain name identifier.
email-address	Clear e-mail address identifier.
firewall-id	Clear Firewall ID identifier.
ipv4	Clear IPv4 address identifier.
ipv6	Clear IPv6 address identifier.
key-id	Clear key ID identifier.

Example

```
no ike-id local email-address
```

Syntax

```
ike-id peer { domain-name <VPN_FQDN> | email-address <EMAIL> | firewall-id <WORD> | ipv4 <IPV4_HOST> | ipv6 <IPV6_HOST> | key-id <WORD> }
```

Mode

IKE Preshared Secret

Description

Configure peer IKE authentication associated identifiers.

Options

domain-name <VPN_FQDN>	Domain name identifier. Domain name in the form: aaa.aa. Example: <i>example.com</i>
email-address <EMAIL>	E-mail address identifier. E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>

<i>firewall-id</i>	Firewall ID identifier.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>ipv4</i>	IP address identifier.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>ipv6</i>	IPv6 address identifier.
<IPV6_HOST>	IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH. Example: <i>2000:0000:0000:ff68:0205:62ef:ee8d:f25b</i>
<i>key-id</i>	Key ID identifier.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
ike-id peer email-address user@domain.com
```

Syntax

```
no ike-id peer { domain-name | email-address | firewall-id | ipv4 | ipv6 | key-id }
```

Mode

IKE Preshared Secret

Description

Clear peer IKE authentication associated identifiers.

Options

<i>domain-name</i>	Clear domain name identifier.
<i>email-address</i>	Clear e-mail address identifier.
<i>firewall-id</i>	Clear Firewall ID identifier.
<i>ipv4</i>	Clear IPv4 address identifier.
<i>ipv6</i>	Clear IPv6 address identifier.
<i>key-id</i>	Clear key ID identifier.

Example

```
no ike-id peer email-address
```

Syntax

```
certificate <CERT_NAME>
```

Mode

IKE 3rd Party Certificate
IKE 3rd Party Certificate
Certificate

Description

Configure the local certificate name.

Options

<CERT_NAME>	Certificate name.

Example: *my_cert*

Example

```
certificate mycertificate
```

Syntax

```
no certificate
```

Mode

IKE 3rd Party Certificate
IKE 3rd Party Certificate
Certificate

Description

Clear the local certificate name.

Example

```
no certificate
```

Syntax

```
ike-id local { default-id | distinguished-name | domain-name | email-id | ip }
```

Mode

IKE 3rd Party Certificate

Description

Configure the local identifier.

Options

<i>default-id</i>	Default ID from the certificate.
<i>distinguished-name</i>	Distinguished name (DN).
<i>domain-name</i>	Domain name (FQDN).
<i>email-id</i>	E-mail ID (userFQDN).
<i>ip</i>	IP address (IPv4).

Example

```
ike-id local default-id
```

Syntax

```
ike-id peer { distinguished-name <DISTINGUISHED_NAME> | domain-name <VPN_FQDN> | email-id <EMAIL> | ip <IPv4_HOST> }
```

Mode

IKE 3rd Party Certificate

Description

Configure the peer identifier.

Options

<i>distinguished-name</i>	Distinguished name (DN).
<DISTINGUISHED_NAME>	Distinguished name filter in the form: c=*;cn=*;o=*;ou=*; or *. Example: <i>ou=aaa;c=a;*</i>
<i>domain-name</i>	Domain name (FQDN).
<VPN_FQDN>	Domain name in the form: aaa.aa. Example: <i>example.com</i>
<i>email-id</i>	E-mail ID (userFQDN).
<EMAIL>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
<i>ip</i>	IP address (IPv4).
<IPv4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
ike-id peer distinguished-name
```

Syntax

```
no ike-id peer { distinguished-name | domain-name | email-id | ip }
```

Mode

IKE 3rd Party Certificate

Description

Clear the peer identifier.

Options

<i>distinguished-name</i>	Clear distinguished name (DN).
<i>domain-name</i>	Clear domain name (FQDN).
<i>email-id</i>	Clear e-mail ID (userFQDN).
<i>ip</i>	Clear IP address (IPv4).

Example

```
no ike-id peer distinguished-name
```

Syntax

```
client-id peer { distinguished-name <DISTINGUISHED_NAME> | domain-name <VPN_FQDN> | email-id <EMAIL> | ip <IPv4_HOST> }
```

Mode

Certificate

Description

Configure the VPN AP client ID.

Options

<i>distinguished-name</i>	Distinguished name (DN).
<DISTINGUISHED_NAME>	Distinguished name filter in the form: c=*;cn=*;o=*;ou=*; or *. Example: <i>ou=aaa;c=a;*</i>
<i>domain-name</i>	Domain name (FQDN).
<VPN_FQDN>	Domain name in the form: aaa.aa. Example: <i>example.com</i>

<i>email-id</i>	E-mail ID (userFQDN).
<i><EMAIL></i>	E-mail in the form: aaaaa@bbb.com. Example: <i>support@sonicwall.com</i>
<i>ip</i>	IP address (IPv4).
<i><IPv4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
client-id peer distinguished-name xxxx
```

Syntax

```
no client-id peer { distinguished-name | domain-name | email-id | ip }
```

Mode

Certificate

Description

Clear the VPN AP client ID.

Options

distinguished-name Clear distinguished name (DN).

domain-name Clear domain name (FQDN).

email-id Clear e-mail ID (userFQDN).

ip Clear IP address (IPv4).

Example

```
no client-id peer distinguished-name
```

Syntax

```
peer id { distinguished-name <DISTINGUISHED_NAME> | domain-name <VPN_FQDN_FILTER> | email-id <VPN_EMAIL_FILTER> }
```

Mode

IKE 3rd Party Certificate

Description

Configure the peer identifier type.

Options

distinguished-name Distinguished name.

<DISTINGUISHED_NAME> Distinguished name filter in the form: c=*;cn=*;o=*;ou=*; or *.
Example: *ou=aaa;c=a;**

domain-name Domain name.

<VPN_FQDN_FILTER> Domain name filter in the form: aabb?*-.aa.
Example: *example.com*

email-id E-mail ID.

<VPN_EMAIL_FILTER> E-mail filter in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

peer id-type domain-name example.com

Syntax

peer match-issuer

Mode

IKE 3rd Party Certificate

Description

Enable allow only peer certificates signed by gateway issuer.

Example

peer match-issuer

Syntax

no peer match-issuer

Mode

IKE 3rd Party Certificate

Description

Disable allow only peer certificates signed by gateway issuer.

Example

no peer match-issuer

Syntax

user-name <WORD>

Mode

SonicWALL auto provisioning client VPN Policy

Description

Set user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name xxxx

Syntax

no user-name

Mode

SonicWALL auto provisioning client VPN Policy

Description

Clear user name.

Example

no user-name

Syntax

user-password <WORD>

Mode

SonicWALL auto provisioning client VPN Policy

Description

Set user password.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

user-password xxxx

Syntax

no user-password

Mode

SonicWALL auto provisioning client VPN Policy

Description

Clear user password.

Example

no user-password

Syntax

network local { allow-unauthenticated { { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | require-xauth <LOCAL_USER_GROUP_NAME> }

Mode

SonicWALL auto provisioning server VPN Policy

Description

Configure the local network.

Options

allow-unauthenticated	Enable unauthenticated access for VPN policy.
group	Configure the remote network to named address object group.
<VPN_ADDR_GROUP_NAME>	Group address object name. Example: Sales Group
host	Host IP.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n

name	Address object name.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Network address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Network range.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
require-xauth	Enable XAUTH checking for VPN policy.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>

Example

```
network local require-xauth "Everyone"
```

Syntax

```
no network local { allow-unauthenticated | require-xauth }
```

Mode

SonicWALL auto provisioning server VPN Policy

Description

Clear the local network user group or unauthenticated network object.

Options

allow-unauthenticated Clear unauthenticated network object.

require-xauth Clear XAUTH user group.

Example

```
no network local allow-unauthenticated
```

Syntax

```
network remote { destination-network { { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | nat-pool { { host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | nat-proxy }
```

Mode

SonicWALL auto provisioning server VPN Policy

Description

Configure the remote network.

Options

destination-network Choose destination network from list.

group Configure the remote network to named address object group.

<VPN_ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Configure the remote network to host address.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Configure the remote network to named address object.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Configure the remote network to network address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Configure the remote network to range of addresses.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
nat-pool	Choose NAT pool.
host	Configure the remote network to host address.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Configure the remote network to named address object.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Configure the remote network to network address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Configure the remote network to range of addresses.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
nat-proxy	Obtain NAT proxy via authentication service.

Example

```
network remote nat-proxy
```

Syntax

```
no network remote { destination-network | nat-pool }
```

Mode

SonicWALL auto provisioning server VPN Policy

Description

Clear the remote network.

Options

destination-network Clear destination network.

nat-pool Clear NAT pool.

Example

```
no network remote destination-network
```

Syntax

```
network local { any | dhcp | group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the local network.

Options

any	Any local network.
dhcp	Obtain IP addresses using DHCP through this VPN tunnel.
group <VPN_ADDR_GROUP_NAME>	Configure the local network to named address object group. Group address object name. Example: <i>Sales Group</i>
host <VPN_ADDR_HOST>	Configure the local network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
name <VPN_ADDR_NAME>	Configure the local network to named address object. Host/network/range address object name. Example: <i>Web Server</i>
network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK>	Configure the local network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <VPN_ADDR_BEGIN> <VPN_ADDR_END>	Configure the local network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
network local name LANSubnets
```

Syntax

```
no network local
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the local network.

Example

```
no network local
```

Syntax

```
network remote { any | destination-network { { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> |  
network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | dhcp | ikev2-ip-pool { { host  
<VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> }  
} }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Configure the remote network.

Options

any	Use this VPN tunnel as default route for all internet traffic.
destination-network	Choose destination network from list.
group <VPN_ADDR_GROUP_NAME>	Configure the remote network to named address object group. Group address object name. Example: <i>Sales Group</i>
host <VPN_ADDR_HOST>	Configure the remote network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <VPN_ADDR_NAME>	Configure the remote network to named address object. Host/network/range address object name. Example: <i>Web Server</i>
network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK>	Configure the remote network to network address. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i> IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <VPN_ADDR_BEGIN> <VPN_ADDR_END>	Configure the remote network to range of addresses. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i> IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
dhcp	Destination network obtains IP addresses using DHCP through this VPN tunnel.
ikev2-ip-pool	Choose NAT pool.
host <VPN_ADDR_HOST>	Configure the remote network to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name <VPN_ADDR_NAME>	Configure the remote network to named address object. Host/network/range address object name. Example: <i>Web Server</i>
network	Configure the remote network to network address.

<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Configure the remote network to range of addresses.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
network remote any
```

Syntax

```
no network remote { destination-network | ikev2-ip-pool }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Clear the remote network.

Options

- destination-network** Clear destination network.
- ikev2-ip-pool** Clear ikev2 IP pool.

Example

```
no network remote destination-network
```

Syntax

```
proposal ike { authentication { { md5 | sha-1 | sha-256 | sha-384 | sha-512 } } | dh-group { { 1 | 14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 } } | encryption { { aes-128 | aes-192 | aes-256 | des | triple-des } } | exchange { { aggressive | ikev2 | main } } | lifetime <UINT32> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Configure VPN policy IKE (phase 1) proposal.

Options

- authentication** Authentication hashing encryption algorithm.
- md5** Message-digest algorithm 5 (MD5).
- sha-1** Secure hash algorithm 1 (SHA-1).
- sha-256** Secure hash algorithm 256 (SHA-256).

<i>sha-384</i>	Secure hash algorithm 384 (SHA-384).
<i>sha-512</i>	Secure hash algorithm 512 (SHA-512).
<i>dh-group</i>	DH group.
<i>1</i>	Group 1 modp768.
<i>14</i>	Group 14 modp2048.
<i>19</i>	Group 19 ECP random 256-bit.
<i>2</i>	Group 2 modp1024.
<i>20</i>	Group 20 ECP random 384-Bit.
<i>21</i>	Group 21 ECP random 521-Bit.
<i>25</i>	Group 25 ECP random 192-Bit.
<i>26</i>	Group 26 ECP random 224-Bit.
<i>5</i>	Group 5 modp1536.
<i>encryption</i>	Encryption algorithm.
<i>aes-128</i>	Advanced encryption standard (AES) - 128 bit.
<i>aes-192</i>	Advanced encryption standard (AES) - 192 bit.
<i>aes-256</i>	Advanced encryption standard (AES) - 256 bit.
<i>des</i>	Data encryption standard (DES).
<i>triple-des</i>	Triple data encryption standard (3DES).
<i>exchange</i>	Exchange.
<i>aggressive</i>	Aggressive mode.
<i>ikev2</i>	IKEv2 mode.
<i>main</i>	Main mode.
<i>lifetime</i>	Life time (seconds).
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
proposal ike encryption aes-256
proposal ike authentication sha-1
proposal ike dh-group 2
proposal ike lifetime 3000
```

Syntax

```
proposal ipsec { authentication { { aes-xcbc | md5 | sha-1 | sha-256 | sha-384 | sha-512 } } | authentication-key
<VPN_HEX_STRING128> | encryption { { aes-128 | aes-192 | aes-256 | aes-gcm16-128 | aes-gcm16-192 | aes-gcm16-256 | aes-gmac-
128 | aes-gmac-192 | aes-gmac-256 | des | triple-des } } | encryption-key <VPN_HEX_STRING128> | in-authentication-key
<VPN_HEX_STRING128> | in-encryption-key <VPN_HEX_STRING128> | in-spi <VPN_HEX_UINT32> | lifebytes <UINT32> | lifetime <UINT32>
| out-authentication-key <VPN_HEX_STRING128> | out-encryption-key <VPN_HEX_STRING128> | out-spi <VPN_HEX_UINT32> | perfect-
forward-secrecy dh-group { { 1 | 14 | 19 | 2 | 20 | 21 | 25 | 26 | 5 } } | protocol { { ah | esp } } }
```

Mode

- Site to Site VPN Policy
- Site to Site VPN IPv6 Policy
- Tunnel Interface VPN Policy

Description

Configure VPN policy IPsec (phase 2) proposal.

Options

<i>authentication</i>	Authentication hashing encryption algorithm.
<i>aes-xcbc</i>	Secure hash algorithm AES (AES-XCBC).
<i>md5</i>	Message-digest algorithm 5 (MD5).
<i>sha-1</i>	Secure hash algorithm 1 (SHA-1).
<i>sha-256</i>	Secure hash algorithm 256 (SHA-256).
<i>sha-384</i>	Secure hash algorithm 384 (SHA-384).
<i>sha-512</i>	Secure hash algorithm 512 (SHA-512).
<i>authentication-key</i> <VPN_HEX_STRING128>	Configure authentication key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
<i>encryption</i>	Encryption algorithm.
<i>aes-128</i>	Advanced encryption standard (AES) - 128 bit.
<i>aes-192</i>	Advanced encryption standard (AES) - 192 bit.
<i>aes-256</i>	Advanced encryption standard (AES) - 256 bit.
<i>aes-gcm16-128</i>	Advanced encryption standard (AES) - GCM16 128 bit.
<i>aes-gcm16-192</i>	Advanced encryption standard (AES) - GCM16 192 bit.
<i>aes-gcm16-256</i>	Advanced encryption standard (AES) - GCM16 256 bit.
<i>aes-gmac-128</i>	Advanced encryption standard (AES) - GMAC 128 bit.
<i>aes-gmac-192</i>	Advanced encryption standard (AES) - GMAC 192 bit.
<i>aes-gmac-256</i>	Advanced encryption standard (AES) - GMAC 256 bit.
<i>des</i>	Data encryption standard (DES).
<i>triple-des</i>	Triple data encryption standard (3DES).
<i>encryption-key</i> <VPN_HEX_STRING128>	Configure encryption key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
<i>in-authentication-key</i> <VPN_HEX_STRING128>	Configure incoming authentication key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
<i>in-encryption-key</i> <VPN_HEX_STRING128>	Configure incoming encryption key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
<i>in-spi</i> <VPN_HEX_UINT32>	Configure incoming SPI. Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i>
<i>lifebytes</i> <UINT32>	Life bytes (kb). Integer in the form: D OR 0xHHHHHHHH.

	Example: <i>123</i>
lifetime <UINT32>	Life time (seconds). Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
out-authentication-key <VPN_HEX_STRING128>	Configure outgoing authentication key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
out-encryption-key <VPN_HEX_STRING128>	Configure outgoing encryption key. String of hexadecimal (16-128) digits. Example: <i>0123456989abcdef</i>
out-spi <VPN_HEX_UINT32>	Configure outgoing SPI. Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i>
perfect-forward-secrecy dh-group	Enable perfect forward secrecy. DH group.
1	Group 1 modp768.
14	Group 14 modp2048.
19	Group 19 ECP random 256-bit.
2	Group 2 modp1024.
20	Group 20 ECP random 384-Bit.
21	Group 21 ECP random 521-Bit.
25	Group 25 ECP random 192-Bit.
26	Group 26 ECP random 224-Bit.
5	Group 5 modp1536.
protocol	Protocol.
ah	Configure AH.
esp	Configure ESP.

Example

```
proposal ipsec encryption aes-256
proposal ipsec authentication sha-1
proposal ipsec perfect-forward-secrecy dh-group 2
proposal ipsec lifetime 3000
proposal ipsec lifebytes 200000
```

Manual Key Only:

```
proposal ipsec in-spi 0x5d1b19a1
proposal ipsec out-spi 0x88f24984
proposal ipsec encryption-key 5f7cd04166523fd78e56ca9920d9c870d53ed63d92001d4f
proposal ipsec authentication-key 3b1db664fe578ae5fd38d7042e7a106f4c23408a
```

Syntax

```
no proposal ipsec { authentication | authentication-key | encryption | encryption-key | lifebytes | perfect-forward-secrecy }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Clear VPN policy IPsec (phase 2) proposal.

Options

<i>authentication</i>	None authentication hashing encryption algorithm.
<i>authentication-key</i>	Configure authentication key.
<i>encryption</i>	None encryption algorithm.
<i>encryption-key</i>	Configure encryption key.
<i>lifebytes</i>	No lifebytes.
<i>perfect-forward-secrecy</i>	Disable perfect forward secrecy.

Example

```
no proposal ipsec encryption-key
no proposal ipsec authentication-key
no proposal ipsec encryption
no proposal ipsec authentication
no proposal ipsec perfect-forward-secrecy
no proposal ipsec lifebytes
```

Syntax

```
client cache-xauth { always | never | single-session }
```

Mode

Group VPN

Description

Configure cache XAUTH user name and password on client.

Options

<i>always</i>	Always cache.
<i>never</i>	No caching.
<i>single-session</i>	Cache for single session.

Example

```
client cache-xauth single-session
```

Syntax

```
client virtual-adaptor { dhcp-and-manual | dhcp-only | none }
```

Mode

Group VPN

Description

Configure virtual adaptor lease settings.

Options

<i>dhcp-and-manual</i>	Use DHCP lease or manual configuration.

<i>dhcp-only</i>	Use DHCP lease.
<i>none</i>	None.

Example

```
client virtual-adaptor dhcp-only
```

Syntax

```
client allow-connections-to { all-secured-gateways | split-tunnels | this-gateway-only }
```

Mode

Group VPN

Description

Configure what connections to allow to.

Options

<i>all-secured-gateways</i>	All secured gateways.
<i>split-tunnels</i>	Split tunnels.
<i>this-gateway-only</i>	This gateway only.

Example

```
client allow-connections-to this-gateway-only
```

Syntax

```
client default-route
```

Mode

Group VPN

Description

Configure default route as this gateway.

Example

```
client default-route
```

Syntax

```
no client default-route
```

Mode

Group VPN

Description

Clear default route as this gateway.

Example

```
no client default-route
```

Syntax

```
client access-list
```

Mode

Group VPN

Description

Enable apply VPN access control list.

Example

```
client access-list
```

Syntax

```
no client access-list
```

Mode

Group VPN

Description

Disable apply VPN access control list.

Example

```
no client access-list
```

Syntax

```
client simple-provisioning
```

Mode

Group VPN

Description

Enable use default key for simple client provisioning.

Example

```
client simple-provisioning
```

Syntax

```
no client simple-provisioning
```

Mode

Group VPN

Description

Disable use default key for simple client provisioning.

Example

```
no client simple-provisioning
```

Syntax

```
keep-alive
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Enable VPN policy keep alive.

Example

```
keep-alive
```

Syntax

```
no keep-alive
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Disable VPN policy keep alive.

Example

```
no keep-alive
```

Syntax

```
suppress-auto-add-rule
```

Mode

Site to Site VPN Policy

Description

Enable suppress automatic access rules creation for VPN policy.

Example

```
suppress-auto-add-rule
```

Syntax

```
no suppress-auto-add-rule
```

Mode

Site to Site VPN Policy

Description

Disable suppress automatic access rules creation for VPN policy.

Example

```
no suppress-auto-add-rule
```

Syntax

```
require-xauth <LOCAL_USER_GROUP_NAME>
```

Mode

Site to Site VPN Policy

Description

Enable XAUTH checking for VPN policy.

Options

<LOCAL_USER_GROUP_NAME> Local user group object name.
Example: *Limited Administrators*

Example

```
require-xauth "Everyone"
```

Syntax

```
no require-xauth
```

Mode

Site to Site VPN Policy

Description

Disable require authentication of VPN clients by XAUTH.

Example

```
no require-xauth
```

Syntax

```
anti-replay
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Enable anti replay.

Example

```
anti-replay
```

Syntax

```
no anti-replay
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Disable anti replay.

Example

no anti-replay

Syntax

advanced-routing

Mode

Tunnel Interface VPN Policy

Description

Enable allow advanced routing.

Example

advanced-routing

Syntax

no advanced-routing

Mode

Tunnel Interface VPN Policy

Description

Disable allow advanced routing.

Example

no advanced-routing

Syntax

transport-mode

Mode

Tunnel Interface VPN Policy

Description

Enable transport mode.

Example

transport-mode

Syntax

no transport-mode

Mode

Tunnel Interface VPN Policy

Description

Disable transport mode.

Example

no transport-mode

Syntax

netbios

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Enable VPN policy NetBIOS.

Example

netbios

Syntax

no netbios

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Disable VPN policy NetBIOS.

Example

no netbios

Syntax

multicast

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Enable VPN policy multicast.

Example

multicast

Syntax

no multicast

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Disable VPN policy multicast.

Example

no multicast

Syntax

permit-acceleration

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Enable permit acceleration.

Example

permit-acceleration

Syntax

no permit-acceleration

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Disable permit acceleration.

Example

no permit-acceleration

Syntax

wxa-group <WXA_GROUP_NAME>

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Configure WXA group.

Options

<WXA_GROUP_NAME> WXA group name.
Example: *Group One*

Example

wxa-group "Group One"

Syntax

no wxa-group

Mode

Description

Clear WXA group.

Example

```
no wxa-group
```

Syntax

```
no translated-network { local | remote }
```

Mode

Site to Site VPN Policy

Description

Clear the translated remote or local network.

Options

local Clear translated local network.

remote Clear translated remote network.

Example

```
no translated-network remote
no translated-network local
```

Syntax

```
translated-network { local { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network
<VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | original | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } | remote { group <VPN_ADDR_GROUP_NAME>
| host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | original | range <VPN_ADDR_BEGIN>
<VPN_ADDR_END> } }
```

Mode

Site to Site VPN Policy

Description

Set translated local or remote network.

Options

local Translated local network.

group Configure the local network to named address object group.

<VPN_ADDR_GROUP_NAME> Group address object name.
Example: *Sales Group*

host Host IP.

<VPN_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form:
HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

name Address object name.

<VPN_ADDR_NAME> Host/network/range address object name.
Example: *Web Server*

network Network address.

<VPN_ADDR_NETWORK> IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form:

	HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original translated local network.
range	Network range.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
remote	Translated remote network.
group	Configure the local network to named address object group.
<VPN_ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
host	Host IP.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
name	Address object name.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
network	Network address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
original	Original translated remote network.
range	Network range.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
translated-network local name "TranslatedLocalAddrs"
translated-network remote name "TranslatedRemoteAddrs"
```

Syntax

```
apply-nat
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Enable apply NAT policies.

Example

```
apply-nat
```

Syntax

no apply-nat

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy

Description

Disable apply NAT policies.

Example

no apply-nat

Syntax

no oosp-checking

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Disable OOSP checking.

Example

no oosp-checking

Syntax

oosp-checking

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Enable and configure OOSP checking.

Example

oosp-checking

Syntax

responder-url <WEB_URL>

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Configure OOSP responder URL.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

responder-url http://www.sonicwall.com/ocsp

Syntax

no responder-url

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
Group VPN

Description

Clear OCSP responder URL.

Example

no responder-url

Syntax

management { http | https | snmp | ssh }

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Enable management for VPN policy.

Options

http Enable HTTP management for VPN policy.

https Enable HTTPS management for VPN policy.

snmp Enable SNMP management for VPN policy.

ssh Enable SSH management for VPN policy.

Example

management https

Syntax

no management { http | https | snmp | ssh }

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Disable management for VPN policy.

Options

- http** Disable HTTP management for VPN policy.
- https** Disable HTTPS management for VPN policy.
- snmp** Disable SNMP management for VPN policy.
- ssh** Disable SSH management for VPN policy.

Example

```
no management https
```

Syntax

```
user-login { http | https }
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Enable VPN policy for user login.

Options

- http** Enable VPN policy for HTTP user login.
- https** Enable VPN policy for HTTPS user login.

Example

```
user-login http
```

Syntax

```
no user-login { http | https }
```

Mode

Site to Site VPN Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Disable VPN policy for user login.

Options

- http** Disable VPN policy for HTTP user login.
- https** Disable VPN policy for HTTPS user login.

Example

```
no user-login http
```

Syntax

```
default-lan-gateway <IPV4_HOST>
```

Mode

Site to Site VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Configure LAN default gateway.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
default-lan-gateway 192.168.168.1
```

Syntax

```
no default-lan-gateway
```

Mode

Site to Site VPN Policy
Group VPN
SonicWALL auto provisioning server VPN Policy

Description

Clear LAN default gateway.

Example

```
no default-lan-gateway
```

Syntax

```
bound-to { interface <VPN_BOUND_TO_INTERFACE> | zone <ZONE_WAN_NAME> }
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Configure VPN policy bound to.

Options

interface Bound to interface.
<VPN_BOUND_TO_INTERFACE> Interface name.
Example: *X0*

zone Bound to zone.
<ZONE_WAN_NAME> Zone object name.
Example: *DMZ*

Example

```
bound-to interface X1
```

Syntax

```
local-ip { custom <IPV6_HOST> | primary }
```

Mode

Description

Set the local gateway ip address.

Options

- custom*

Specify the Local Gateway IP address.
- <IPv6_HOST>*

IPv6 Address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH.
Example: *2000:0000:0000:ff68:0205:62ef:ee8d:f25b*
- primary*

Using Primary IP address.

Example

local-ip custom 4::5

Syntax

preempt-secondary-gateway <UINT32>

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Enable preempt secondary gateway and set primary gateway detection interval (seconds).

Options

- <UINT32>*

Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

preempt-secondary-gateway 28800

Syntax

no preempt-secondary-gateway

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy

Description

Disable preempt secondary gateway.

Example

no preempt-secondary-gateway

Syntax

client-authentication { allow-unauthenticated { { group <VPN_ADDR_GROUP_NAME> | host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } } | require-xauth <LOCAL_USER_GROUP_NAME> }

Mode

Group VPN

Description

Enable XAUTH checking for VPN policy.

Options

<i>allow-unauthenticated</i>	Enable unauthenticated access for VPN policy.
<i>group</i>	Configure the remote network to named address object group.
<VPN_ADDR_GROUP_NAME>	Group address object name. Example: <i>Sales Group</i>
<i>host</i>	Host IP.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address object name.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
<i>network</i>	Network address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Network range.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>require-xauth</i>	Enable XAUTH checking for VPN policy.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>

Example

client-authentication require-xauth "Everyone"

Syntax

suppress-trigger-packet

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not send trigger packet during IKE SA negotiation for IKEv2.

Example

suppress-trigger-packet

Syntax

no suppress-trigger-packet

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Send trigger packet during IKE SA negotiation for IKEv2.

Example

```
no suppress-trigger-packet
```

Syntax

```
accept-hash
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Accept hash & URL certificate type for IKEv2.

Example

```
accept-hash
```

Syntax

```
no accept-hash
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not accept hash & URL certificate type for IKEv2.

Example

```
no accept-hash
```

Syntax

```
send-hash <WEB_URL>
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Enable send hash & URL certificate type for IKEv2 and specify url.

Options

<WEB_URL> URL in the form: http://host/file.
Example: *http://www.example.com/products/*

Example

```
send-hash <ikev2CertUrl>
```

Syntax

no send-hash

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy

Description

Do not send hash & URL certificate type for IKEv2.

Example

no send-hash

Syntax

accept-multiple-proposals

Mode

Group VPN

Description

Enable accept multiple proposals for clients.

Example

accept-multiple-proposals

Syntax

no accept-multiple-proposals

Mode

Group VPN

Description

Disable accept multiple proposals for clients.

Example

no accept-multiple-proposals

Syntax

ike-mode-configuration { expiry-time <UINT32> | ip-pool { host <VPN_ADDR_HOST> | name <VPN_ADDR_NAME> | network <VPN_ADDR_NETWORK> <VPN_ADDR_MASK> | range <VPN_ADDR_BEGIN> <VPN_ADDR_END> } }

Mode

Group VPN

Description

Enable IKE Mode Configuration.

Options

<i>expiry-time</i>	Address Expiry Time(seconds).
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

<i>ip-pool</i>	IP Pool for Clients.
<i>host</i>	Host IP.
<VPN_ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>name</i>	Address Object name.
<VPN_ADDR_NAME>	Host/network/range address object name. Example: <i>Web Server</i>
<i>network</i>	Network Address.
<VPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<VPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
<i>range</i>	Network Range.
<VPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<VPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
ike-mode-configuration ip-pool name "IpPoolClientAdrrs"
ike-mode-configuration expiry-time 3600
```

Syntax

```
no ike-mode-configuration
```

Mode

Group VPN

Description

Disable IKE Mode Configuration.

Example

```
no ike-mode-configuration
```

Syntax

```
allow-sonicpointn-layer3
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Allow SonicPointN layer 3 management.

Example

```
allow-sonicpointn-layer3
```

Syntax

```
no allow-sonicpointn-layer3
```

Mode

Site to Site VPN Policy
Site to Site VPN IPv6 Policy
Tunnel Interface VPN Policy
SonicWALL auto provisioning server VPN Policy

Description

Disallow SonicPointN layer 3 management.

Example

```
no allow-sonicpointn-layer3
```

Syntax

```
l2tp-server
```

Mode

VPN

Description

Enter L2TP server configure mode.

Example

```
l2tp-server
```

Syntax

```
enable
```

Mode

L2TP Server

Description

Enable L2TP Server.

Example

```
enable
```

Syntax

```
no enable
```

Mode

L2TP Server

Description

Disable L2TP Server.

Example

```
no enable
```

Syntax

```
keep-alive <UINT32>
```

Mode

L2TP Server

Description

Set the Keep alive time (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

keep-alive 10

Syntax

dns { primary <IPV4_HOST> | secondary <IPV4_HOST> }

Mode

L2TP Server

Description

Set the primary and secondary DNS server IP address.

Options

primary Primary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

secondary Secondary DNS server IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

dns primary 192.168.168.169

Syntax

no dns { primary | secondary }

Mode

L2TP Server

Description

Manually Clear DNS server IP address.

Options

primary Clear primary DNS server IP address.

secondary Clear secondary DNS server IP address.

Example

no dns primary

Syntax

```
wins { primary <IPv4_HOST> | secondary <IPv4_HOST> }
```

Mode

L2TP Server

Description

Set the WINS server IP address.

Options

<i>primary</i>	Primary WINS server IP address.
<i><IPv4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>secondary</i>	Secondary WINS server IP address.
<i><IPv4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins { primary | secondary }
```

Mode

L2TP Server

Description

Clear the WINS server IP address.

Options

<i>primary</i>	Primary WINS server IP address.
<i>secondary</i>	Secondary WINS server IP address.

Example

```
no wins primary
```

Syntax

```
ip-pool { local <IPv4_HOST> <IPv4_HOST> | provided }
```

Mode

L2TP Server

Description

Set the IP address pool.

Options

<i>local</i>	Use local L2TP IP pool.
<i><IPv4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i><IPv4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>provided</i>	IP address provided by RADIUS/LDAP Server.

Example

```
ip-pool local 192.168.168.10 192.168.168.20
```

Syntax

```
no user-group
```

Mode

L2TP Server

Description

No L2TP user group.

Example

```
no user-group
```

Syntax

```
user-group <LOCAL_USER_GROUP_NAME>
```

Mode

L2TP Server

Description

Set user group for L2TP users.

Options

- <LOCAL_USER_GROUP_NAME>** Local user group object name.
Example: *Limited Administrators*

Example

```
user-group l2tpUsers
```

Syntax

```
ppp protocol { chap | mschap | mschapv2 | pap } order <UINT8>
```

Mode

L2TP Server

Description

Set PPP authentication protocol and enter the configuration mode.

Options

- chap** CHAP
- mschap** MSCHAP
- mschapv2** MSCHAPv2
- pap** PAP
- order** PPP authentication protocol order.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: *123*

Example


```
authentication-protocol pap order 1
```

Syntax

```
no ppp protocol { chap | mschap | mschapv2 | pap }
```

Mode

L2TP Server

Description

Remove specified PPP authentication protocol.

Options

chap PAP

mschap PAP

mschapv2 PAP

pap PAP

Example

```
no authentication-protocol pap
```

Syntax

```
no ppp protocols
```

Mode

L2TP Server

Description

Remove all PPP authentication protocol.

Example

```
no authentication-protocols
```

Syntax

```
disconnect session <IPv4_HOST>
```

Mode

L2TP Server

Description

Disconnect l2tp session.

Options

<IPv4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
disconnect session 3.3.3.3
```

Syntax

dhcp-over-vpn

Mode

VPN

Description

Configure DHCP over VPN and enter dhcp over vpn mode.

Example

dhcp-over-vpn

Syntax

clear lease <IPV4_HOST>

Mode

DHCP over vpn

Description

Delete DHCP over VPN lease.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

clear lease 1.1.1.1

Syntax

clear leases

Mode

DHCP over vpn

Description

Delete all DHCP over VPN lease.

Example

clear leases

Syntax

mode { central | remote }

Mode

DHCP over vpn

Description

Configure DHCP over VPN mode.

Options

central Central gateway.

remote Remote gateway.

Example

```
mode central
```

Syntax

```
central
```

Mode

DHCP over vpn

Description

Configure DHCP over VPN for central gateway and enter to central mode.

Example

```
central
```

Syntax

```
remote
```

Mode

DHCP over vpn

Description

Configure DHCP over VPN for remote gateway and enter to remote mode.

Example

```
remote
```

Syntax

```
internal-dhcp
```

Mode

Central

Description

Enable use internal DHCP server.

Example

```
internal-dhcp
```

Syntax

```
no internal-dhcp
```

Mode

Central

Description

Disable use internal DHCP server.

Example

```
no internal-dhcp
```

Syntax

```
global-vpn
```

Mode

Central

Description

Enable use internal DHCP server for global VPN client.

Example

```
global-vpn
```

Syntax

```
no global-vpn
```

Mode

Central

Description

Disable use internal DHCP server for global VPN client.

Example

```
no global-vpn
```

Syntax

```
remote
```

Mode

Central

Description

Enable use internal DHCP server for remote firewall.

Example

```
remote
```

Syntax

```
no remote
```

Mode

Central

Description

Disable use internal DHCP server for remote firewall.

Example

```
no remote
```

Syntax

send-requests

Mode

Central

Description

Enable send DHCP requests to the server addresses in the server list.

Example

send-requests

Syntax

no send-requests

Mode

Central

Description

Disable send DHCP requests to the server addresses in the server list.

Example

no send-requests

Syntax

dhcp-server <DHCP_SERVER_IPV4_HOST>

Mode

Central

Description

Add/edit a DHCP server to the server list and enter to configuration mode.

Options

<DHCP_SERVER_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

dhcp-server 192.168.168.170

Syntax

no dhcp-server <DHCP_SERVER_IPV4_HOST>

Mode

Central

Description

Remove a DHCP server from the server list.

Options

<DHCP_SERVER_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
no dhcp-server 192.168.168.170
```

Syntax

```
no dhcp-servers
```

Mode

Central

Description

Remove all DHCP servers from the server list.

Example

```
no dhcp-servers
```

Syntax

```
ip <IPV4_HOST>
```

Mode

DHCP server

Description

Ip address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ip 192.168.168.170
```

Syntax

```
no relay-ip
```

Mode

Central

Description

Clear DHCP relay IP address.

Example

```
no relay-ip
```

Syntax

```
relay-ip <IPV4_HOST>
```

Mode

Central

Description

Configure DHCP relay IP address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
relay-ip 192.168.168.170
```

Syntax

```
bound-to <DHCP_OVER_VPN_INTERFACE>
```

Mode

Remote

Description

DHCP lease bound to.

Options

<DHCP_OVER_VPN_INTERFACE> Interface name.
Example: *X0*

Example

```
bound-to X2
```

Syntax

```
accept-bridged-wlan-request
```

Mode

Remote

Description

Accept DHCP request from bridged WLAN interface.

Example

```
accept-bridged-wlan-request
```

Syntax

```
no accept-bridged-wlan-request
```

Mode

Remote

Description

Reject DHCP request from bridged WLAN interface.

Example

```
no accept-bridged-wlan-request
```

Syntax

```
no relay-ip
```

Mode

Remote

Description

Clear DHCP relay IP address.

Example

```
no relay-ip
```

Syntax

```
relay-ip <IPV4_HOST>
```

Mode

Remote

Description

Configure DHCP relay IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
relay-ip 192.168.168.170
```

Syntax

```
no management-ip
```

Mode

Remote

Description

Clear remote management IP address.

Example

```
no management-ip
```

Syntax

```
management-ip <IPV4_HOST>
```

Mode

Remote

Description

Configure remote management IP address.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
management-ip 192.168.168.170
```

Syntax

```
block-spoof
```

Mode

Remote

Description

Enable block traffic through tunnel when IP spoof detected.

Example

```
block-spoof
```

Syntax

```
no block-spoof
```

Mode

Remote

Description

Disable block traffic through tunnel when IP spoof detected.

Example

```
no block-spoof
```

Syntax

```
temp-lease
```

Mode

Remote

Description

Enable obtain temporary lease from local DHCP server if tunnel is down.

Example

```
temp-lease
```

Syntax

```
no temp-lease
```

Mode

Remote

Description

Disable obtain temporary lease from local DHCP server if tunnel is down.

Example

```
no temp-lease
```

Syntax

lease-time <UINT8>

Mode

Remote

Description

Set the temporary lease time (minutes).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

lease-time 10

Syntax

static-device <STATIC_DEVICE_IPV4_HOST>

Mode

Remote

Description

Add/edit a static devices on LAN and enter to configuration mode.

Options

<STATIC_DEVICE_IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

static-device 192.168.168.170

Syntax

no static-device <STATIC_DEVICE_IPV4_HOST>

Mode

Remote

Description

Remove a static device on LAN.

Options

<STATIC_DEVICE_IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

no static-device 192.168.168.170

Syntax

no static-devices

Mode

Remote

Description

Remove all static devices on LAN.

Example

no static-devices

Syntax

ip <IPV4_HOST>

Mode

Static device

Description

Ip address.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

ip 192.168.168.170

Syntax

mac <MAC>

Mode

Static device

Description

MAC address.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

mac 01:02:03:04:05:06

Syntax

excluded-device <EXCLUDE_DEVICE_MAC>

Mode

Remote

Description

Add/edit an excluded LAN device and enter to configuration mode.

Options

<EXCLUDE_DEVICE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

excluded-device 01:02:03:04:05:06

Syntax

no excluded-device <EXCLUDE_DEVICE_MAC>

Mode

Remote

Description

Remove an excluded LAN device.

Options

<EXCLUDE_DEVICE_MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

no excluded-device 01:02:03:04:05:06

Syntax

no excluded-devices

Mode

Remote

Description

Remove all excluded LAN devices.

Example

no excluded-devices

Syntax

mac <MAC>

Mode

Exclude device

Description

MAC address.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

mac 01:02:03:04:05:06

Syntax

```
clear dhcp-servers
```

Mode

Central

Description

DHCP over VPN delete all DHCP servers.

Example

```
clear dhcp-servers
```

Syntax

```
clear static-devices
```

Mode

Remote

Description

DHCP over VPN delete all static devices.

Example

```
clear static-devices
```

Syntax

```
clear excluded-lan-devices
```

Mode

Remote

Description

DHCP over VPN delete all exclded lan devices.

Example

```
clear excluded-lan-devices
```

Syntax

```
show vpn [ { { tunnel <VPN_POLICY_NAME> | tunnels } [ ike | ipsec | summary ] } | base | dhcp-over-vpn [ { base { { central | global | remote } } | dhcp-server <DHCP_SERVER_IPV4_HOST> | dhcp-servers | excluded-device <EXCLUDE_DEVICE_MAC> | excluded-devices | leases [ ip <IPV4_HOST> ] | static-device <STATIC_DEVICE_IPV4_HOST> | static-devices | statistics } ] | l2tp-server [ base | ppp ] [ sessions ] | policies [ { ipv4 [ { group-vpn | provision-client | provision-server | site-to-site | tunnel-interface } ] | ipv6 [ site-to-site ] } ] | policy { ipv4 { { group-vpn <VPN_GROUP_POLICY_NAME> | provision-client <VPN_PROVISION_CLIENT_POLICY_NAME> | provision-server <VPN_PROVISION_SERVER_POLICY_NAME> | site-to-site <VPN_SITE_POLICY_NAME> | tunnel-interface <VPN_TUNNEL_POLICY_NAME> } } | ipv6 { site-to-site <VPN_SITE_POLICY_V6_NAME> } } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show VPN status or configuration.

Options

tunnel	Show an active VPN tunnel.
<VPN_POLICY_NAME>	VPN policy name.

	Example: <i>Remote Office</i>
tunnels	Show all currently active VPN tunnels.
ike	Show ike sa.
ipsec	Show ipsec sa.
summary	Show vpn sa number.
base	Show VPN base settings.
dhcp-over-vpn	Show DHCP over VPN status or configuration.
base	Show DHCP over VPN base settings.
central	Show DHCP over VPN central gateway base settings.
global	Show DHCP over VPN global base settings.
remote	Show DHCP over VPN remote gateway base settings.
dhcp-server <DHCP_SERVER_IPV4_HOST>	Add a DHCP server to the server list. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
dhcp-servers	Show DHCP over VPN dhcp servers.
excluded-device <EXCLUDE_DEVICE_MAC>	Add an excluded LAN device. MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
excluded-devices	Show DHCP over VPN excluded devices.
leases ip <IPV4_HOST>	Show DHCP over VPN leases. DHCP over VPN lease ip. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
static-device <STATIC_DEVICE_IPV4_HOST>	Add a static devices on LAN. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
static-devices	Show DHCP over VPN static devices.
statistics	Show DHCP over VPN current lease counts.
l2tp-server	Show L2TP server configuration.
base	Show L2TP server base settings.
ppp sessions	Show L2TP server PPP settings. Show L2TP server active sessions.
policies	Show all VPN policies.
ipv4	Show only IPv4 VPN policies.
group-vpn	Show only IPv4 group VPN policies.
provision-client	Show SonicWALL auto provisioning client VPN policy.
provision-server	Show SonicWALL auto provisioning server VPN policy.
site-to-site	Show only IPv4 site to site VPN policies.
tunnel-interface	Show only IPv4 tunnel interface VPN policies.

ipv6	Show only IPv6 VPN policies.
site-to-site	Show only IPv6 site to site VPN policies.
policy	Show a VPN policy.
ipv4	IPv4 VPN policy.
group-vpn	Show IPv4 group VPN policy.
<VPN_GROUP_POLICY_NAME>	Group VPN policy name. Example: <i>WAN GroupVPN</i>
provision-client	Show SonicWALL auto provisioning client VPN policy.
<VPN_PROVISION_CLIENT_POLICY_NAME>	SonicWALL auto provisioning client VPN policy name. Example: <i>SonicWALL auto provision client Policy</i>
provision-server	Show SonicWALL auto provisioning server VPN policy.
<VPN_PROVISION_SERVER_POLICY_NAME>	SonicWALL auto provisioning server VPN policy name. Example: <i>SonicWALL auto provision server Policy</i>
site-to-site	Show IPv4 site to site VPN policy.
<VPN_SITE_POLICY_NAME>	Site-to-site VPN policy name. Example: <i>Remote Office</i>
tunnel-interface	Show IPv4 tunnel interface VPN policy.
<VPN_TUNNEL_POLICY_NAME>	Tunnel interface VPN policy name. Example: <i>Remote Office</i>
ipv6	IPv6 VPN policy.
site-to-site	IPv6 site-to-site VPN policy.
<VPN_SITE_POLICY_V6_NAME>	IPv6 Site-to-site VPN policy name. Example: <i>Remote Office</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show vpn
show vpn tunnels
show vpn tunnel "Remote Office"
show vpn tunnels ipsec
show vpn statistics 0x23ab3456
show vpn dhcp-over-vpn
show vpn dhcp-over-vpn leases
show vpn l2tp-server
show vpn policy ipv4 tunnel-interface "Remote Office"
show vpn policies
```

Syntax

```
ssl-vpn server
```

Mode

Config

Description

Configure SSL VPN server settings.

Example

```
ssl-vpn server
```

Syntax

```
logout <SSLVPN_LOGOUT_IPV4_HOST>
```

Mode

SSL VPN Server

Description

Logout specified NetExtender virtual IP.

Options

<SSLVPN_LOGOUT_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

logout 1.1.1.1

Syntax

access [enable] <SSLVPN_ZONE_NAME>

Mode

SSL VPN Server

Description

Enable SSL VPN access on specified zone.

Options

enable Enable SSL VPN access on specified zone.
<SSLVPN_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

access WAN

Syntax

no access [enable] <SSLVPN_ZONE_NAME>

Mode

SSL VPN Server

Description

Disable SSL VPN access on specified zone.

Options

enable Disable SSL VPN access on specified zone.
<SSLVPN_ZONE_NAME> Zone object name.
Example: *DMZ*

Example

no access WAN

Syntax

port <IPV4_PORT>

Mode

SSL VPN Server

Description

Set SSL VPN server port.

Options

<IPV4_PORT> Integer in the form: D OR 0xHHHH.
Example: *80*

Example

```
port 4433
```

Syntax

```
certificate { name <CERT_NAME> | use-self-signed }
```

Mode

SSL VPN Server

Description

Select SSL certificate to use for SSL VPN.

Options

name Specify certificate.

<CERT_NAME> Certificate name.
Example: *my_cert*

use-self-signed Use self signed certificate.

Example

```
certificate name CorpSSLVPCert
```

Syntax

```
use-radius { mschap | mschapv2 }
```

Mode

SSL VPN Server

Description

Enable use RADIUS in specified mode for XAUTH.

Options

mschap Use MSCHAP for RADIUS.

mschapv2 Use MSCHAPv2 for RADIUS.

Example

```
use-radius mschapv2
```

Syntax

```
no use-radius
```

Mode

SSL VPN Server

Description

Disable use RADIUS for XAUTH.

Example

```
no use-radius
```

Syntax

```
user-domain <HOSTNAME>
```

Mode

SSL VPN Server

Description

Set user domain.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
user-domain LocalDomain
```

Syntax

```
no user-domain
```

Mode

SSL VPN Server

Description

Clear user domain.

Example

```
no user-domain
```

Syntax

```
management web
```

Mode

SSL VPN Server

Description

Enable web management over SSL VPN.

Example

```
management web
```

Syntax

```
no management web
```

Mode

SSL VPN Server

Description

Disable web management over SSL VPN.

Example

```
no management web
```

Syntax

```
management ssh
```

Mode

SSL VPN Server

Description

Enable SSH management over SSL VPN.

Example

```
management ssh
```

Syntax

```
no management ssh
```

Mode

SSL VPN Server

Description

Disable SSH management over SSL VPN.

Example

```
no management ssh
```

Syntax

```
session-timeout <UINT32>
```

Mode

SSL VPN Server

Description

Set the default session timeout in minutes.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
session-timeout 10
```

Syntax

```
inactivity-check
```

Mode

SSL VPN Server

Description

Enable SSL VPN inactivity check.

Example

```
inactivity-check
```

Syntax

```
no inactivity-check
```

Mode

SSL VPN Server

Description

Disable SSL VPN inactivity check.

Example

```
no inactivity-check
```

Syntax

```
download-url { custom <WORD> | default }
```

Mode

SSL VPN Server

Description

Set SSL VPN client download URL.

Options

custom Manually specify SSL VPN image URL.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

default Enable use default SSL VPN image URL.

Example

```
download-url default
```

Syntax

```
ssl-vpn portal
```

Mode

Config

Description

Configure SSL VPN portal settings.

Example

```
ssl-vpn portal
```

Syntax

site-title <WORD>

Mode

SSL VPN Portal

Description

Set SSL VPN portal site title.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

site-title "Corp - Virtual Office"

Syntax

banner-title <WORD>

Mode

SSL VPN Portal

Description

Set SSL VPN portal banner title.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

banner-title "Virtual Office"

Syntax

home-page-message { *custom* <ROL> | *default* }

Mode

SSL VPN Portal

Description

Set SSL VPN portal home page message.

Options

custom Use customized home page message.
<ROL> Remaining command line input.
Example: *line...*

default Use default home page message example template.

Example

home-page-message custom "TBD"

Syntax

```
login-message { custom <ROL> | default }
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal login message.

Options

<i>custom</i>	Use customized login message.
<i><ROL></i>	Remaining command line input. Example: <i>line...</i>
<i>default</i>	Use default login message example template.

Example

```
login-message custom "TBD"
```

Syntax

```
auto-launch
```

Mode

SSL VPN Portal

Description

Enable launch NetExtender after login.

Example

```
auto-launch
```

Syntax

```
no auto-launch
```

Mode

SSL VPN Portal

Description

Disable launch NetExtender after login.

Example

```
no auto-launch
```

Syntax

```
cache-control
```

Mode

SSL VPN Portal

Description

Enable HTTP meta tags for cache control (recommended).

Example

```
cache-control
```

Syntax

```
no cache-control
```

Mode

SSL VPN Portal

Description

Disable HTTP meta tags for cache control (recommended).

Example

```
no cache-control
```

Syntax

```
display-link
```

Mode

SSL VPN Portal

Description

Enable display UTM management link on SSL VPN portal(not recommended).

Example

```
display-link
```

Syntax

```
no display-link
```

Mode

SSL VPN Portal

Description

Disable display UTM management link on SSL VPN portal(not recommended).

Example

```
no display-link
```

Syntax

```
logo { custom <SSLVPN_LOGO> | default }
```

Mode

SSL VPN Portal

Description

Set SSL VPN portal logo.

Options

custom	Enable use custom sonicwall logo.
<SSLVPN_LOGO>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>/VirtulOffice.gif</i>
default	Enable use default sonicwall logo.

Example

logo default

Syntax

ssl-vpn epc-profile

Mode

Config

Description

Configure SSL VPN EPC profile.

Example

ssl-vpn epc-profile

Syntax

ssl-vpn profile

Mode

Config

Description

Configure SSL VPN default device profile.

Example

ssl-vpn profile

Syntax

enable-epc

Mode

EPC Profile

Description

Enable EPC.

Example

enable-epc

Syntax

no enable-epc

Mode

EPC Profile

Description

Disable EPC.

Example

```
no enable-epc
```

Syntax

```
fallback-options { default | quarantine }
```

Mode

EPC Profile

Description

Device profile fallback options.

Options

default Place into default device profile.

quarantine Place into quarantine device profile.

Example

```
fallback-options default
```

Syntax

```
device-profile <EPC_DEVICE_NAME>
```

Mode

Default Device Profile

Description

Configure default device profile.

Options

<EPC_DEVICE_NAME> Device name in the form: WORD or \"QUOTED STRING\".
Example: *Default Device Profile*

Example

```
device-profile "Default Device Profile"  
device-profile "Default Device Profile for SonicPointN"
```

Syntax

```
device-profile { linux | macos | windows } name <EPC_DEVICE_NAME>
```

Mode

EPC Profile

Description

Configure device profile.

Options

linux The operation system type of profile is linux

macos	The operation system type of profile is macos
windows	The operation system type of profile is windows
name	Name of the profile.
<EPC_DEVICE_NAME>	Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i>

Example

```
device-profile windows name "Default Device Profile for Windows"
```

Syntax

```
no device-profile { linux | macos | windows } name <EPC_DEVICE_NAME>
```

Mode

EPC Profile

Description

Delete the device profile.

Options

linux	OsType of device is linux
macos	OsType of device is macos
windows	OsType of device is windows
name	Name of the device profile.
<EPC_DEVICE_NAME>	Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i>

Example

```
no device-profile windows name "Default Device Profile for Windows"
```

Syntax

```
no device-profiles { linux | macos | windows }
```

Mode

EPC Profile

Description

Delete all device profiles which os type is window, linux or macos.

Options

linux	OsType of device is linux
macos	OsType of device is macos
windows	OsType of device is windows

Example

```
no device-profiles windows
```

Syntax

name <WORD>

Mode

Device Profile

Description

Configure name for the device profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name device1

Syntax

description <WORD>

Mode

Device Profile

Description

Configure description for the device profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

description "device desc1-desc"

Syntax

no description

Mode

Device Profile

Description

Clear device description.

Example

no description

Syntax

enable

Mode

Device Profile

Description

Enable the device profile.

Example

enable

Syntax

no enable

Mode

Device Profile

Description

Disable the device profile.

Example

no enable

Syntax

action { allow | deny }

Mode

Device Profile

Description

Configure action for the device profile.

Options

allow Device is allowed.

deny Device is denied.

Example

action allow

Syntax

network-address { ipv4 | ipv6 } { host <SSLVPN_ADDR_HOST> | name <SSLVPN_ADDR_NAME> | network <SSLVPN_ADDR_NETWORK> <SSLVPN_ADDR_MASK> | range <SSLVPN_ADDR_BEGIN> <SSLVPN_ADDR_END> } [zone <SSLVPN_ADDR_ZONE_NAME>]

Mode

Device Profile

Description

Setting network address for the client device.

Options

ipv4 Set IPv4 address object for the device profile.

ipv6 Set IPv6 address object for the device profile.

host Configure address object using host name.
<SSLVPN_ADDR_HOST> IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

name Address object name.
<SSLVPN_ADDR_NAME> Host/network/range address object name.

Example: *Web Server*

network	Configure address object using network.
<SSLVPN_ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<SSLVPN_ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Configure address object using range.
<SSLVPN_ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<SSLVPN_ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
zone	Set SSL VPN zone object.
<SSLVPN_ADDR_ZONE_NAME>	Zone object name. Example: <i>SSLVPN</i>

Example

```
network-address ipv4 name addr
network-address ipv4 host 192.168.168.33
network-address ipv4 range 192.168.100.50 192.168.100.60
network-address ipv4 network 192.168.100.0 /24
network-address ipv4 network 192.168.100.0 255.255.255.0
network-address ipv6 name addr
network-address ipv6 host fe10::1001
network-address ipv6 range fe10::1001 fe10::1100
network-address ipv6 network fe10::1001 /64
```

Syntax

```
no network-address { ipv4 | ipv6 }
```

Mode

Device Profile

Description

Clear network address for client device.

Options

ipv4 Clear IPv4 network address for the device profile.

ipv6 Clear IPv6 network address for the device profile.

Example

```
no network-address ipv4
no network-address ipv6
```

Syntax

```
deny-message <WORD>
```

Mode

Device Profile

Description

Configure message for the deny device.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
deny-message "some msg"
```

Syntax

```
no deny-message
```

Mode

Device Profile

Description

Clear message for the deny device.

Example

```
no deny-message
```

Syntax

```
quarantine-message { custom <WORD> | default }
```

Mode

Device Profile

Description

Configure message for a quarantine device.

Options

custom	Set message customer value.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
default	Set message default value.

Example

```
quarantine-message custom "some msg"
```

Syntax

```
no quarantine-message
```

Mode

Device Profile

Description

Clear quarantine message for the quarantine device.

Example

```
no quarantine-message
```

Syntax

```
wlan-tunnel-interface <WLAN_TUNNEL_INTERFACE>
```

Mode

Device Profile

Description

Configure wlan tunnel interface for SonicPointN L3 profile.

Options

<WLAN_TUNNEL_INTERFACE> WLAN tunnel interface name.
Example: *WT0*

Example

wlan-tunnel-interface X1

Syntax

no wlan-tunnel-interface

Mode

Device Profile

Description

Clear wlan tunnel interface for SonicPointN L3 profile.

Example

no wlan-tunnel-interface

Syntax

security

Mode

Device Profile

Description

Security related config for the device profile.

Example

security

Syntax

routes

Mode

Device Profile

Description

Routes related config for the device profile.

Example

routes

Syntax

client

Mode

Device Profile

Description

Client related config for the device profile.

Example

client

Syntax

no all-attributes

Mode

Device Profile Security

Description

Delete all security attribute.

Example

no all-attributes

Syntax

type { anti-spyware | anti-virus } { vendor <SSLVPN_SECURITY_VENDOR> [product <SSLVPN_SECURITY_PRODUCT> [[version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER>] [updated-operator <OPERAND> updated-days <UINT32>] [scanned-operator <OPERAND> scanned-days <UINT32>] [realtime]]] }

Mode

Device Profile Security

Description

Add a security attribute of type antivirus program or antispyware program.

Options

anti-spyware	Add a security attribute of type antispyware program.
anti-virus	Add a security attribute of type antivirus program.
vendor	The vendor of antivirus program or antispyware program.
<SSLVPN_SECURITY_VENDOR>	Antivirus Program. Example: <i>Kaspersky Labs</i>
product	The product name of antivirus program or antispyware program.
<SSLVPN_SECURITY_PRODUCT>	Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i>
version-operator	Product version.
<OPERAND>	Operand. Example: = != >= > <= <
version	Product version.
<SSLVPN_SECURITY_PRODUCT_VER>	Antivirus Program Product Version. Example: <i>2.x</i>
updated-operator	Signature updated date.
<OPERAND>	Operand. Example: = != >= > <= <
updated-days	Signature updated date.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
scanned-operator	File system scanned date.
<OPERAND>	Operand. Example: = != >= > <= <
scanned-days	File system scanned date.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH.

Example: *123*

realtime

Realtime protection required.

Example

```
type anti-virus vendor "firewall name" product "product name" version-operator > version 4.0 updated-operator > updated-days 30 scanned-operator < scanned-days 25 realtime
```

Syntax

```
no type { anti-spyware | anti-virus } { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] [ updated-operator <OPERAND> updated-days <UINT32> ] [ scanned-operator <OPERAND> scanned-days <UINT32> ] [ realtime ] ] ] }
```

Mode

Device Profile Security

Description

Delete a security attribute of type antivirus program or antispyware program.

Options

<i>anti-spyware</i>	Delete a security attribute of type antispyware program.
<i>anti-virus</i>	Delete a security attribute of type antivirus program.
<i>vendor</i>	The vendor of antivirus program or antispyware program.
<i><SSLVPN_SECURITY_VENDOR></i>	Antivirus Program. Example: <i>Kaspersky Labs</i>
<i>product</i>	The product name of antivirus program ,antispyware program or firewall.
<i><SSLVPN_SECURITY_PRODUCT></i>	Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i>
<i>version-operator</i>	Product version.
<i><OPERAND></i>	Operand. Example: = != >= > <= <
<i>version</i>	Product version.
<i><SSLVPN_SECURITY_PRODUCT_VER></i>	Antivirus Program Product Version. Example: <i>2.x</i>
<i>updated-operator</i>	Signature updated date.
<i><OPERAND></i>	Operand. Example: = != >= > <= <
<i>updated-days</i>	Signature updated date.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>scanned-operator</i>	File system scanned date.
<i><OPERAND></i>	Operand. Example: = != >= > <= <
<i>scanned-days</i>	File system scanned date.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>realtime</i>	Realtime protection required.

Example

```
no anti-virus vendor "firewall name" product "product name" version-operator > version 4.0 updated-operator > updated-days 30 scanned-operator < scanned-days 25 realtime
```

Syntax

```
firewall { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ version-operator <OPERAND> version <SSLVPN_SECURITY_PRODUCT_VER> ] ] }
```

Mode

Device Profile Security

Description

Add a security attribute of type personal firewall program.

Options

vendor	The vendor of antivirus program ,antispysware program or firewall.
<SSLVPN_SECURITY_VENDOR>	Antivirus Program. Example: <i>Kaspersky Labs</i>
product	The product of antivirus program ,antispysware program or firewall.
<SSLVPN_SECURITY_PRODUCT>	Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i>
version-operator	Product version.
<OPERAND>	Operand. Example: = != >= > <= <
version	Product version.
<SSLVPN_SECURITY_PRODUCT_VER>	Antivirus Program Product Version. Example: <i>2.x</i>

Example

```
firewall vendor "firewall name" product "product name" version-operator > version 4.0
```

Syntax

```
no firewall { vendor <SSLVPN_SECURITY_VENDOR> [ product <SSLVPN_SECURITY_PRODUCT> [ version-operator <OPERAND> version  
<SSLVPN_SECURITY_PRODUCT_VER> ] ] }
```

Mode

Device Profile Security

Description

Delete a security attribute of type personal firewall program.

Options

vendor	The vendor of antivirus program, antispysware program or firewall.
<SSLVPN_SECURITY_VENDOR>	Antivirus Program. Example: <i>Kaspersky Labs</i>
product	The product of antivirus program, antispysware program or firewall.
<SSLVPN_SECURITY_PRODUCT>	Antivirus Program Product. Example: <i>Kaspersky Anti-Virus 2009</i>
version-operator	Configure SSL VPN.
<OPERAND>	Operand. Example: = != >= > <= <
version	Product version.
<SSLVPN_SECURITY_PRODUCT_VER>	Antivirus Program Product Version. Example: <i>2.x</i>

Example

```
no firewall vendor "firewall name" product "product name" version-operator > version 4.0
```

Syntax

```
certification <SSLVPN_SECURITY_CERT> search { system-only | system-user }
```

Mode

Device Profile Security

Description

Add a security attribute of type certification.

Options

<SSLVPN_SECURITY_CERT>	Client Certification. Example: <i>Certification xxx.</i>
search	Look for the certification.

<i>system-only</i>	Look in system store only.
<i>system-user</i>	Look in system store and user store.

Example

certification certName search system-only

Syntax

no certification

Mode

Device Profile Security

Description

Delete a security attribute of type certification.

Example

no certification

Syntax

application <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type application.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

application app-name

Syntax

no application <WORD>

Mode

Device Profile Security

Description

Delete a security attribute of type application.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no application app-name

Syntax

directory <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type directory name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

directory dir-name

Syntax

no directory <WORD>

Mode

Device Profile Security

Description

Delete a security attribute of type directory name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no directory dir-name

Syntax

equipment <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type equipment identifier.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

equipment equip-id

Syntax

no equipment

Mode

Description

Delete a security attribute of type equipment identifier.

Example

no equipment

Syntax

domain <WORD>

Mode

Device Profile Security

Description

Add a security attribute of type windows domain.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

domain domain-name

Syntax

no domain

Mode

Device Profile Security

Description

Delete a security attribute of type windows domain.

Example

no domain

Syntax

file file-name <WORD> [size-operator <OPERAND> bytes <UINT32>] [date-operator <OPERAND> [date { absolute <DATE_YYYYMMDD> | relative days <UINT32> }] [time <TIME_HHMMSS>]] [validate { md5 <WORD> | windows }]

Mode

Device Profile Security

Description

Add a security attribute of type file name.

Options

file-name	File name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
size-operator	File size is bigger or less .etc.
<OPERAND>	Operand. Example: = != >= > <= <
bytes	File size.

<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
date-operator	
<OPERAND>	Operand. Example: = != >= > <= <
date	Last modified.
absolute	Absolute date.
<DATE_YYYYMMDD>	Date in the form: YYYY:MM:DD. Example: <i>2010:06:30</i>
relative	Relative date.
days	
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
time	Set relative time.
<TIME_HHMMSS>	Time in the form: DD:DD:DD. Example: <i>12:00:00</i>
validate	Validate file integrity.
md5	Use MD5 or SHA-1 hash.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
windows	Use windows catalog file.

Example

```
file file-name fileName1 size-operator > bytes 2 date-operator < date absolute 2011/11/11 time 11:11:11 validate windows
```

Syntax

```
no file file-name <WORD> [ size-operator <OPERAND> bytes <UINT32> ] [ date-operator <OPERAND> [ date { absolute <DATE_YYYYMMDD> | relative days <UINT32> } ] ] [ time <TIME_HHMMSS> ] ] [ validate { md5 <WORD> | windows } ]
```

Mode

Device Profile Security

Options

file-name	File name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
size-operator	File size is bigger or less .etc.
<OPERAND>	Operand. Example: = != >= > <= <
bytes	File size.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
date-operator	
<OPERAND>	Operand. Example: = != >= > <= <
date	Last modified.
absolute	Absolute date.
<DATE_YYYYMMDD>	Date in the form: YYYY:MM:DD. Example: <i>2010:06:30</i>
relative	Relative date.
days	
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
time	Set relative time.
<TIME_HHMMSS>	Time in the form: DD:DD:DD. Example: <i>12:00:00</i>
validate	Validate file integrity.
md5	Use MD5 or SHA-1 hash.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

windows Use windows catalog file.

Example

```
no file file-name fileName1 size-operator > bytes 2 date-operator < date absolute 2011/11/11 time 11:11:11 validate windows
```

Syntax

```
registry key <WORD> [ value <WORD> ] [ data-operator <OPERAND> data <WORD> ]
```

Mode

Device Profile Security

Description

Add a security attribute of type windows registry entry.

Options

key	Key of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
value	Value of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
data-operator	Registry entry.
<OPERAND>	Operand. Example: = != >= > <= <
data	Data of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
registry key keyname value valuenam data-operator > data abcd
```

Syntax

```
no registry key <WORD> [ value <WORD> ] [ data-operator <OPERAND> data <WORD> ]
```

Mode

Device Profile Security

Description

Delete a security attribute of type windows registry entry.

Options

key	Key of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
value	Value of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
data-operator	Registry entry.
<OPERAND>	Operand. Example: = != >= > <= <
data	Data of the registry entry.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
no registry key keyname value valuenam data-operator = data abcd
```

Syntax

```
os-version <OS_VERSION> [ build <UINT32> ] [ version-operator <OPERAND> ]
```

Mode

Device Profile Security

Description

Add a security attribute of type windows version.

Options

<OS_VERSION>	Operation System Version. Example: <i>windows 7</i>
build	Build of windows version.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
version-operator	
<OPERAND>	Operand. Example: <i>= != >= > <= <</i>

Example

```
os-version windows-xp build 2345 version-operator >
```

Syntax

```
no os-version <OS_VERSION> [ build <UINT32> ] [ version-operator <OPERAND> ]
```

Mode

Device Profile Security

Description

Delete a security attribute of type windows version.

Options

<OS_VERSION>	Operation System Version. Example: <i>windows 7</i>
build	Build of windows version.
<UINT32>	Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
version-operator	
<OPERAND>	Operand. Example: <i>= != >= > <= <</i>

Example

```
no os-version windows-xp build 2345 version-operator >
```

Syntax

```
dns inherit
```

Mode

Device Profile Client

Description

Set DNS server IP address for NetExtender client.

Example

```
dns inherit
```

Syntax

```
dns primary <IP_V4V6_HOST>
```

Mode

Device Profile Client

Description

Set the primary DNS server IP address for NetExtender client.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
dns primary 192.168.168.170
dns primary fe80::1002
```

Syntax

```
no dns primary
```

Mode

Device Profile Client

Description

Clear the primary DNS server IP address for NetExtender client.

Example

```
no dns primary
```

Syntax

```
dns secondary <IP_V4V6_HOST>
```

Mode

Device Profile Client

Description

Set the secondary DNS server IP address for NetExtender client.

Options

<IP_V4V6_HOST> IPV4: address in the form: D.D.D.D\nIPV6: address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: 2001:cdba:0000:0000:0000:0000:3257:9652

Example

```
dns secondary 192.168.168.170
dns secondary fe80::1002
```

Syntax

```
no dns secondary
```

Mode

Device Profile Client

Description

Clear the secondary DNS server IP address for NetExtender client.

Example

```
no dns secondary
```

Syntax

```
dns search-list <HOSTNAME>
```

Mode

Device Profile Client

Description

Add a dns to the dns search list.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
dns search-list 192.168.168.169
```

Syntax

```
no dns search-list <HOSTNAME>
```

Mode

Device Profile Client

Description

Clear a dns from the dns search list.

Options

<HOSTNAME> Hostname in the form: hostname OR a.b.c.d.
Example: *example.com*

Example

```
no dns search-list 192.168.168.169
```

Syntax

```
no dns search-lists
```

Mode

Device Profile Client

Description

Clear all dns from the dns search list.

Example

```
no dns search-lists
```

Syntax

```
wins primary <IPV4_HOST>
```

Mode

Device Profile Client

Description

Set the primary WINS server IP address for NetExtender clients.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins primary 192.168.168.169
```

Syntax

```
no wins primary
```

Mode

Device Profile Client

Description

Clear the primary WINS server IP address for NetExtender clients.

Example

```
no wins primary
```

Syntax

```
wins secondary <IPV4_HOST>
```

Mode

Device Profile Client

Description

Set the secondary WINS server IP address for NetExtender clients.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
wins secondary 192.168.168.170
```

Syntax

```
no wins secondary
```

Mode

Device Profile Client

Description

Clear the secondary WINS server IP address for NetExtender clients.

Example

no wins secondary

Syntax

auto-update

Mode

Device Profile Client

Description

Enable client auto update.

Example

auto-update

Syntax

no auto-update

Mode

Device Profile Client

Description

Disable client auto update.

Example

no auto-update

Syntax

exit-after-disconnect

Mode

Device Profile Client

Description

Enable exit client after disconnect.

Example

exit-after-disconnect

Syntax

no exit-after-disconnect

Mode

Device Profile Client

Description

Disable exit client after disconnect.

Example

no exit-after-disconnect

Syntax

```
netbios-over-sslvpn
```

Mode

Device Profile Client

Description

Enable NetBIOS over SSL VPN.

Example

```
netbios-over-sslvpn
```

Syntax

```
no netbios-over-sslvpn
```

Mode

Device Profile Client

Description

Disable NetBIOS over SSL VPN.

Example

```
no netbios-over-sslvpn
```

Syntax

```
touch-id-authentication
```

Mode

Device Profile Client

Description

Allow Touch ID on IOS devices.

Example

```
touch-id-authentication
```

Syntax

```
no touch-id-authentication
```

Mode

Device Profile Client

Description

Disable allow Touch ID on IOS devices.

Example

```
no touch-id-authentication
```

Syntax

```
fingerprint-authentication
```

Mode

Device Profile Client

Description

Allow fingerprint authentication on Android devices.

Example

```
fingerprint-authentication
```

Syntax

```
no fingerprint-authentication
```

Mode

Device Profile Client

Description

Disable allow fingerprint authentication on Android devices.

Example

```
no fingerprint-authentication
```

Syntax

```
uninstall-after-exit
```

Mode

Device Profile Client

Description

Enable uninstall client after exit.

Example

```
uninstall-after-exit
```

Syntax

```
no uninstall-after-exit
```

Mode

Device Profile Client

Description

Disable uninstall client after exit.

Example

```
no uninstall-after-exit
```

Syntax

```
create-connection-profile
```

Mode

Device Profile Client

Description

Enable create client connection profile.

Example

```
create-connection-profile
```

Syntax

```
no create-connection-profile
```

Mode

Device Profile Client

Description

Disable create client connection profile.

Example

```
no create-connection-profile
```

Syntax

```
cache { credentials | user-name-only }
```

Mode

Device Profile Client

Description

Set user name and password caching.

Options

credentials Allow saving of user name and password.

user-name-only Allow saving of user name only.

Example

```
cache user-name-only
```

Syntax

```
no cache
```

Mode

Device Profile Client

Description

Prohibit saving of user name and password.

Example

```
no cache
```

Syntax

```
tunnel-all
```

Mode

Device Profile Routes

Description

Enable tunnel all.

Example

tunnel-all

Syntax

no tunnel-all

Mode

Device Profile Routes

Description

Disable tunnel all.

Example

no tunnel-all

Syntax

route [ipv4 | ipv6] { group <SSLVPN_ROUTES_ADDR_GROUP_NAME> | name <SSLVPN_ROUTES_ADDR_NAME> }

Mode

Device Profile Routes

Description

Add a client route.

Options

<i>ipv4</i>	IPv4.
<i>ipv6</i>	IPv6.
<i>group</i> <i><SSLVPN_ROUTES_ADDR_GROUP_NAME></i>	Add an address group to client route. SSLVPN Route Address Group name. Example: <i>Sales Group</i>
<i>name</i> <i><SSLVPN_ROUTES_ADDR_NAME></i>	Add an address object to client route. SSLVPN Route Address Object name. Example: <i>Web Server</i>

Example

route name "Corp SSL-VPN Servers"
route ipv6 name myV6AddrObj

Syntax

no route [ipv4 | ipv6] { group <SSLVPN_ROUTES_ADDR_GROUP_NAME> | name <SSLVPN_ROUTES_ADDR_NAME> }

Mode

Device Profile Routes

Description

Delete a client route.

Options

<i>ipv4</i>	IPv4.
<i>ipv6</i>	IPv6.
<i>group</i> <SSLVPN_ROUTES_ADDR_GROUP_NAME>	Delete an address group to client route. SSLVPN Route Address Group name. Example: <i>Sales Group</i>
<i>name</i> <SSLVPN_ROUTES_ADDR_NAME>	Delete an address object to client route. SSLVPN Route Address Object name. Example: <i>Web Server</i>

Example

no route name "Corp SSL-VPN Servers"
no route ipv6 name myV6AddrObj

Syntax

no routes

Mode

Device Profile Routes

Description

Delete all client routes.

Example

no routes

Syntax

ssl-vpn virtual-office

Mode

Config

Description

Configure SSL VPN virtual office settings.

Example

ssl-vpn virtual-office

Syntax

ssl-vpn logout <SSLVPN_LOGOUT_IPV4_HOST>

Mode

Config

Description

Logout specified NetExtender virtual IP.

Options

<SSLVPN_LOGOUT_IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ssl-vpn logout 1.1.1.1
```

Syntax

```
bookmark <SSLVPN_BOOKMARK>
```

Mode

Virtual Office

Description

Add/edit bookmark and enter configuration mode.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
bookmark "Admin Desktop"
```

Syntax

```
no bookmark <SSLVPN_BOOKMARK>
```

Mode

Virtual Office

Description

Delete a specified bookmark.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no bookmark "Admin Work Desktop"
```

Syntax

```
no bookmarks
```

Mode

Virtual Office

Description

Delete all bookmarks.

Example

```
no bookmarks
```

Syntax

name <SSLVPN_BOOKMARK>

Mode

Bookmark

Description

Set bookmark name.

Options

<SSLVPN_BOOKMARK> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Admin Work Desktop"

Syntax

host <WORD>

Mode

Bookmark

Description

Set host name or IP address.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

host 192.168.168.57

Syntax

no host

Mode

Bookmark

Description

Clear host name or IP address.

Example

no host

Syntax

service { rdp | sshv2 | telnet | vnc }

Mode

Bookmark

Description

Set bookmark service type.

Options

<i>rdp</i>	Terminal services (RDP-HTML5).
<i>sshv2</i>	Secure shell version 2 (SSHv2).
<i>telnet</i>	Telnet.
<i>vnc</i>	Virtual network computing (VNC).

Example

```
service vnc
```

Syntax

```
screen-size { 1024x768 | 1280x1024 | 640x480 | 800x600 | full-screen }
```

Mode

RDP

Description

Set screen size.

Options

<i>1024x768</i>	1024x768.
<i>1280x1024</i>	1280x1024.
<i>640x480</i>	640x480.
<i>800x600</i>	800x600.
<i>full-screen</i>	Full screen.

Example

```
screen-size 1024x768
```

Syntax

```
colors { 15bit | 16bit | 24bit | 256 | 32bit }
```

Mode

RDP

Description

Set screen colors.

Options

<i>15bit</i>	15 bit - high color.
<i>16bit</i>	16 bit - high color.
<i>24bit</i>	24 bit - high color.
<i>256</i>	256 bit.
<i>32bit</i>	32 bit - highest quality.

Example

```
colors 24bit
```

Syntax

```
application-path <WORD>
```

Mode

RDP

Description

Set application and path to launch.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
application-path "C:\\\\Remote Applications\\\\myapp.exe"
```

Syntax

```
no application-path
```

Mode

RDP

Description

Clear application and path.

Example

```
no application-path
```

Syntax

```
start-in-folder <WORD>
```

Mode

RDP

Description

Set folder to start in.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
start-in-folder "C:\\Work\\"
```

Syntax

```
no start-in-folder
```

Mode

RDP

Description

Clear folder to start in.

Example

```
no start-in-folder
```

Syntax

```
automatic-login { custom [ name <WORD> ] [ password <ENC_PASSWORD> ] [ domain <WORD> ] | ssl-vpn }
```

Mode

RDP

Description

Enable automatically log in.

Options

custom	Use custom account credentials.
name	Enter login name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
password	Enter login password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>
domain	Enter login domain.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
ssl-vpn	Use SSL-VPN account credentials.

Example

```
automatic-login custom name myuser password mypassword domain mydomain
```

Syntax

```
no automatic-login [ custom { domain | name | password } ]
```

Mode

RDP

Description

Disable automatically log in.

Options

custom	Use custom account credentials.
domain	Clear login domain.
name	Clear login name.
password	Clear login password.

Example

```
no automatic-login  
no automatic-login custom name
```

```
no automatic-login custom password
no automatic-login custom domain
```

Syntax

```
redirect-clipboard
```

Mode

RDP

Description

Enable redirect clipboard.

Example

```
redirect-clipboard
```

Syntax

```
no redirect-clipboard
```

Mode

RDP

Description

Disable redirect clipboard.

Example

```
no redirect-clipboard
```

Syntax

```
redirect-audio
```

Mode

RDP

Description

Enable redirect audio.

Example

```
redirect-audio
```

Syntax

```
no redirect-audio
```

Mode

RDP

Description

Disable redirect audio.

Example

```
no redirect-audio
```

Syntax

auto-reconnection

Mode

RDP

Description

Enable automatic reconnection.

Example

auto-reconnection

Syntax

no auto-reconnection

Mode

RDP

Description

Disable automatic reconnections.

Example

no auto-reconnection

Syntax

desktop-background

Mode

RDP

Description

Enable desktop background.

Example

desktop-background

Syntax

no desktop-background

Mode

RDP

Description

Disable desktop background.

Example

no desktop-background

Syntax

window-drag

Mode

RDP

Description

Enable window drag.

Example

window-drag

Syntax

no window-drag

Mode

RDP

Description

Disable window drag.

Example

no window-drag

Syntax

animation

Mode

RDP

Description

Enable menu / window animation.

Example

animation

Syntax

no animation

Mode

RDP

Description

Disable menu / window animation.

Example

no animation

Syntax

view-only

Mode

VNC

Description

Enable view only.

Example

view-only

Syntax

no view-only

Mode

VNC

Description

Disable view only.

Example

no view-only

Syntax

share-desktop

Mode

VNC

Description

Enable share desktop.

Example

share-desktop

Syntax

no share-desktop

Mode

VNC

Description

Disable share desktop.

Example

no share-desktop

Syntax

automatic-accept-host-key

Mode

SSHV2

Description

Enable automatically accept host key.

Example

```
automatic-accept-host-key
```

Syntax

```
no automatic-accept-host-key
```

Mode

SSHV2

Description

Disable automatically accept host key.

Example

```
no automatic-accept-host-key
```

Syntax

```
display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Enable display bookmark to mobile connect clients.

Example

```
display-on-mobile
```

Syntax

```
no display-on-mobile
```

Mode

RDP
SSHV2
VNC
Telnet

Description

Disable display bookmark to mobile connect clients.

Example

```
no display-on-mobile
```

Syntax

```
show ssl-vpn [ bookmark <SSLVPN_BOOKMARK> | bookmarks [ sessions ] | device-profile <EPC_DEVICE_NAME> | device-profiles | epc-profile [ { { { linux | macos | windows } name <EPC_DEVICE_NAME> } | base } ] | epc-profiles | portal | server [ { accesses | base } ] | sessions | statistics <SSLVPN_LOGOUT_IPV4_HOST> ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show SSL VPN status or configuration.

Options

bookmark <SSLVPN_BOOKMARK>	Show a specified virtual office bookmark. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
bookmarks	Show all virtual office bookmarks.
sessions	Show all active bookmark sessions.
device-profile <EPC_DEVICE_NAME>	Show default device profile configuration. Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i>
device-profiles	Show all default device profiles configuration.
epc-profile	Show EPC profile configuration.
linux	Show linux EPC profile configuration.
macos	Show macos EPC profile configuration.
windows	Show windows EPC profile configuration.
name <EPC_DEVICE_NAME>	Show EPC profile configuration. Device name in the form: WORD or \"QUOTED STRING\". Example: <i>Default Device Profile</i>
base	Show EPC profile base configuration.
epc-profiles	Show all EPC profiles configuration.
portal	Show portal configuration.
server	Show server configuration.
accesses	Show server accesses configuration.
base	Show server base configuration.
sessions	Show all active sslvpn sessions.
statistics <SSLVPN_LOGOUT_IPV4_HOST>	Show statistics for the session associated with the specified netextender virtual IP. IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

show ssl-vpn

Syntax

high-availability

Mode

Config

Description

Enter high availability configuration mode.

Example

```
high-availability
```

Syntax

```
heartbeat-interval <UINT32>
```

Mode

High Availability

Description

Set heartbeat interval in milliseconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
heartbeat-interval 5000
```

Syntax

```
failover-trigger-level <UINT8>
```

Mode

High Availability

Description

Set failover trigger level (missed heartbeats).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
failover-trigger-level 5
```

Syntax

```
probe interval <UINT8>
```

Mode

High Availability

Description

Set probe interval in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

probe interval 20

Syntax

probe count <UINT8>

Mode

High Availability

Description

Set probe count.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

probe count 3

Syntax

election-delay-time <UINT8>

Mode

High Availability

Description

Set election delay time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

election-delay-time 3

Syntax

route-hold-down-time <UINT8>

Mode

High Availability

Description

Set dynamic route hold-down time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

route-hold-down-time 3

Syntax

```
no route-hold-down-time
```

Mode

High Availability

Description

Clear dynamic route hold-down time.

Example

```
no route-hold-down-time
```

Syntax

```
sdwan-hold-down-time <UINT8>
```

Mode

High Availability

Description

Set SD-WAN probes hold-down time in seconds.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
sdwan-hold-down-time 3
```

Syntax

```
failover-when-aggregate-down
```

Mode

High Availability

Description

Enable failover only when all aggregate links are down.

Example

```
failover-when-aggregate-down
```

Syntax

```
no failover-when-aggregate-down
```

Mode

High Availability

Description

Disable failover only when all aggregate links are down.

Example

```
no failover-when-aggregate-down
```

Syntax

include-certificates-keys

Mode

High Availability

Description

Enable include certificates and keys.

Example

include-certificates-keys

Syntax

no include-certificates-keys

Mode

High Availability

Description

Disable include certificates and keys.

Example

no include-certificates-keys

Syntax

synchronize settings

Mode

High Availability

Description

Synchronize settings.

Example

synchronize settings

Syntax

synchronize firmware

Mode

High Availability

Description

Synchronize firmware.

Example

synchronize firmware

Syntax

force-failover

Mode

High Availability

Description

Force HA active/standby failover.

Example

force-failover

Syntax

no mode

Mode

High Availability

Description

Disable high availability.

Example

no mode

Syntax

mode { active-active-dpi | active-standby }

Mode

High Availability

Description

Enable high availability and set high availability mode.

Options

active-active-dpi Active-active DPI mode.

active-standby Active-standby mode.

Example

mode active-standby

Syntax

primary-serial <MAC>

Mode

Active Standby
Active Active Dpi

Description

Set high availability primary serial number.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
primary-serial 0017C5010203
```

Syntax

```
secondary-serial <MAC>
```

Mode

Active Standby
Active Active Dpi

Description

Set high availability secondary serial number.

Options

<MAC> MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
secondary-serial 0017C5040506
```

Syntax

```
no secondary-serial
```

Mode

Active Standby
Active Active Dpi

Description

Clear high availability secondary serial number.

Example

```
no secondary-serial
```

Syntax

```
stateful-synchronization
```

Mode

Active Standby

Description

Enable stateful synchronization.

Example

```
stateful-synchronization
```

Syntax

```
no stateful-synchronization
```

Mode

Active Standby

Description

Disable stateful synchronization.

Example

```
no stateful-synchronization
```

Syntax

```
dpi-interface <DPI_INTERFACE_ID> <HA_DATA_INTERFACE>
```

Mode

Active Active Dpi

Description

Configure active/active DPI interface.

Options

<DPI_INTERFACE_ID>	Integer in the form: D OR 0xHH. Example: <i>1</i>
<HA_DATA_INTERFACE>	Interface name. Example: <i>X0</i>

Example

```
dpi-interface 1 X5
```

Syntax

```
no dpi-interface <DPI_INTERFACE_ID>
```

Mode

Active Active Dpi

Description

Clear active/active DPI interface.

Options

<DPI_INTERFACE_ID>	Integer in the form: D OR 0xHH. Example: <i>1</i>

Example

```
no dpi-interface 1
```

Syntax

```
control-interface <HA_LINK_INTERFACE>
```

Mode

Active Standby
Active Active Dpi

Description

Configure HA control interface.

Options

<HA_LINK_INTERFACE>	Interface name. Example: <i>X0</i>

Example

```
control-interface X5
```

Syntax

```
no control-interface
```

Mode

Active Standby
Active Active Dpi

Description

Clear HA control interface.

Example

```
no control-interface
```

Syntax

```
data-interface <HA_DATA_INTERFACE>
```

Mode

Active Standby
Active Active Dpi

Description

Configure HA data interface.

Options

<HA_DATA_INTERFACE> Interface name.
Example: *X0*

Example

```
data-interface X5
```

Syntax

```
no data-interface
```

Mode

Active Standby
Active Active Dpi

Description

Clear HA data interface.

Example

```
no data-interface
```

Syntax

```
preempt
```

Mode

Active Standby
Active Active Dpi

Description

Enable preempt mode.

Example

preempt

Syntax

no preempt

Mode

Active Standby
Active Active Dpi

Description

Disable preempt mode.

Example

no preempt

Syntax

encryption

Mode

Active Standby
Active Active Dpi

Description

Enable encryption for control communication.

Example

encryption

Syntax

no encryption

Mode

Active Standby
Active Active Dpi

Description

Disable encryption for control communication.

Example

no encryption

Syntax

virtual-mac

Mode

Active Standby
Active Active Dpi

Description

Enable virtual MAC.

Example

virtual-mac

Syntax

no virtual-mac

Mode

Active Standby
Active Active Dpi

Description

Disable virtual MAC.

Example

no virtual-mac

Syntax

monitoring

Mode

High Availability

Description

High availability monitoring.

Example

monitoring

Syntax

monitoring interface [ipv4 | ipv6] <HA_MONITOR_INTERFACE>

Mode

High Availability

Description

Enter high availability monitoring configuration mode.

Options

ipv4	High availability monitoring interface IPv4.
ipv6	High availability monitoring interface IPv6.
<HA_MONITOR_INTERFACE>	HA monitoring interface name. Example: <i>X0</i>

Example

monitoring interface X1

Syntax

link-monitoring

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable physical/link monitoring.

Example

link-monitoring

Syntax

no link-monitoring

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable physical/link monitoring.

Example

no link-monitoring

Syntax

no primary

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Clear primary interface monitoring IP address.

Example

no primary

Syntax

primary <HOST_IP>

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Set primary interface monitoring IP address.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

Example

```
primary fe80::1001
primary 192.168.168.211
```

Syntax

no secondary

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Clear secondary interface monitoring IP address.

Example

```
no secondary
```

Syntax

secondary <HOST_IP>

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Set secondary interface monitoring IP address.

Options

<HOST_IP> IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n*

Example

```
secondary fe80::1001
secondary 192.168.168.211
```

Syntax

allow-management

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable allow management on primary/secondary IP address.

Example

```
allow-management
```

Syntax

no allow-management

Mode

Description

Disable allow management on primary/secondary IP address.

Example

```
no allow-management
```

Syntax

```
logical-probe { enable | ip <HOST_IP> }
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Enable logical/probe and set IP address.

Options

enable	Enable logical/probe.
ip	Set logical/probe ip.
<HOST_IP>	IPv4: IPv4 host address in the form: D.D.D.D\nIPv6: IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>

Example

```
logical-probe ip fe80::1001  
logical-probe ip 192.168.168.211
```

Syntax

```
no logical-probe { enable | ip }
```

Mode

High Availability Monitoring
High Availability Monitoring IPv6

Description

Disable logical/probe.

Options

enable	Disable logical/probe.
ip	Clear logical/probe IP.

Example

```
no logical-probe enable
```

Syntax

```
override-virtual-mac { enable | mac <MAC> }
```

Mode

Description

Enable override virtual MAC and set MAC.

Options

- enable** Enable logical/probe.
- mac** MAC.
- <MAC>** MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

override-virtual-mac mac 02:17:c5:01:02:03

Syntax

no override-virtual-mac { enable | mac }

Mode

Description

Disable override virtual MAC.

Options

- enable** Disable override virtual MAC.
- mac** Disable override virtual MAC.

Example

no override-virtual-mac enable

Syntax

show high-availability [base | monitoring [ipv4 | ipv6] [interface <HA_MONITOR_INTERFACE>] | status] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show high availability configuration and status.

Options

- base** Show high availability base status.
- monitoring** Show high availability monitoring interface.
- ipv4** Show only IPv4 high availability monitoring interface.
- ipv6** Show only IPv6 high availability monitoring interface.
- interface** Show high availability monitoring interface.
- <HA_MONITOR_INTERFACE>** HA monitoring interface name.
Example: *X0*

<i>status</i>	Show high availability status.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show high-availability
```

Syntax

```
sla-class-object <SDWAN_SLA_CLASS_OBJECT_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN SLA Class Object.

Options

<SDWAN_SLA_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

```
sla-class-object "VoIP"
```

Syntax

```
no sla-class-object <SDWAN_SLA_CLASS_OBJECT_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN SLA Class Object.

Options

<SDWAN_SLA_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

```
no sla-class-object "Best of All"
```

Syntax

```
no sla-class-objects
```

Mode

SD-WAN

Description

Delete all SD-WAN SLA Class Objects.

Example

```
no sla-class-objects
```

Syntax

name <SDWAN_SLA_CLASS_OBJECT_NAME>

Mode

SD-WAN SLA Class Object

Description

Set SD-WAN SLA Class Object name.

Options

<SDWAN_SLA_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

name "Best of All"

Syntax

include { jitter | latency | packet-loss }

Mode

SD-WAN SLA Class Object

Description

Include latency/jitter/packet-loss.

Options

jitter Include jitter.

latency Include latency.

packet-loss Include packet loss.

Example

include jitter

Syntax

no include { jitter | latency | packet-loss }

Mode

SD-WAN SLA Class Object

Description

Disable include latency/jitter/packet-loss.

Options

jitter Include jitter.

latency Include latency.

packet-loss Include packet loss.

Example

```
no include jitter
```

Syntax

```
latency <DECIMAL>
```

Mode

SD-WAN SLA Class Object

Description

Set latency in millisecond.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
latency 8
```

Syntax

```
no latency
```

Mode

SD-WAN SLA Class Object

Description

Clear latency.

Example

```
no latency
```

Syntax

```
jitter <DECIMAL>
```

Mode

SD-WAN SLA Class Object

Description

Set jitter in millisecond.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
jitter 10
```

Syntax

```
no jitter
```

Mode

SD-WAN SLA Class Object

Description

Clear jitter.

Example

```
no jitter
```

Syntax

```
packet-loss <DECIMAL>
```

Mode

SD-WAN SLA Class Object

Description

Set packet loss in percentage.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

```
packet-loss 20
```

Syntax

```
no packet-loss
```

Mode

SD-WAN SLA Class Object

Description

Clear packet loss.

Example

```
packet-loss 20
```

Syntax

```
comment <WORD>
```

Mode

SD-WAN SLA Class Object

Description

Set comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
comment myObject
```

Syntax

no comment

Mode

SD-WAN SLA Class Object

Description

Clear comment.

Example

no comment

Syntax

sla-probe <SDWAN_PROBE_NAME>

Mode

SD-WAN

Description

Add/edit a SD-WAN SLA Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

sla-probe "Remote Servers"

Syntax

no sla-probe <SDWAN_PROBE_NAME>

Mode

SD-WAN

Description

Delete SD-WAN SLA Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

no sla-probe "Remote Servers"

Syntax

no sla-probes [ipv4]

Mode

SD-WAN

Description

Delete all SD-WAN SLA Probes.

Options

ipv4 Delete IPv4 network monitor policies.

Example

```
no sla-probes
```

Syntax

```
name <SDWAN_PROBE_NAME>
```

Mode

SD-WAN SLA Probe

Description

Edit a SD-WAN SLA Probe name.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

Example

```
name "Remote Servers"
```

Syntax

```
sdwan-group <SDWAN_PROBE_GROUP_NAME>
```

Mode

SD-WAN SLA Probe

Description

Edit a SD-WAN SLA Probe interface group.

Options

<SDWAN_PROBE_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
group "VoIP"
```

Syntax

```
no probe target
```

Mode

SD-WAN SLA Probe

Description

Clear the probe target.

Example

```
no probe target
```

Syntax

```
probe target { fqdn <ADDR_FQDN> | host <ADDR_HOST> | name <ADDR_FQDNHOST_ADDR> }
```

Mode

SD-WAN SLA Probe

Description

Set the probe target.

Options

<i>fqdn</i> <ADDR_FQDN>	Set the probe target to FQDN address. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>host</i> <ADDR_HOST>	Set the probe target to host address. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<i>name</i> <ADDR_FQDNHOST_ADDR>	Set the probe target to named address object. FQDN/host address object name. Example: <i>Web Server</i>

Example

```
probe target name "Remote Target"
```

Syntax

```
probe type { ping explicit | tcp explicit port <IPV4_PORT> }
```

Mode

SD-WAN SLA Probe

Description

Set SD-WAN SLA Probe type.

Options

<i>ping</i>	Ping probe.
<i>explicit</i>	Ping probe using explicit route.
<i>tcp</i>	TCP probe.
<i>explicit</i>	TCP probe using explicit route.
<i>port</i>	Set TCP probe port.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
probe type ping explicit
probe type tcp explicit port 80
```

Syntax

```
probe interval <UINT16>
```

Mode

SD-WAN SLA Probe

Description

Set probe host interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
probe interval 5
```

Syntax

```
reply-timeout <UINT8>
```

Mode

SD-WAN SLA Probe

Description

Set probing reply timeout.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
reply-timeout 2
```

Syntax

```
interval missed <UINT8>
```

Mode

SD-WAN SLA Probe

Description

Probe state is set to DOWN after specified number of missed intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interval missed 3
```

Syntax

```
interval successful <UINT8>
```

Mode

SD-WAN SLA Probe

Description

Probe state is set to UP after specified number of successful intervals.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interval successful 3
```

Syntax

```
rst-as-miss
```

Mode

SD-WAN SLA Probe

Description

Enable RST response counts as miss.

Example

```
rst-as-miss
```

Syntax

```
no rst-as-miss
```

Mode

SD-WAN SLA Probe

Description

Disable RST response counts as miss.

Example

```
no rst-as-miss
```

Syntax

```
comment <WORD>
```

Mode

SD-WAN SLA Probe

Description

Set SD-WAN SLA Probe comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Remote Servers"
```

Syntax

```
no comment
```

Mode

SD-WAN SLA Probe

Description

Clear SD-WAN SLA Probe comment.

Example

```
no comment
```

Syntax

```
sdwan
```

Mode

Config

Description

Enter SD-WAN configuration mode.

Example

```
sdwan
```

Syntax

```
no group <SDWAN_GROUP_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN Group.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
no group "VoIP"
```

Syntax

```
no groups
```

Mode

SD-WAN

Description

Delete all SD-WAN groups.

Example

```
no groups
```

Syntax

```
group <SDWAN_GROUP_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN Group.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
group "VoIP"
```

Syntax

```
name <SDWAN_GROUP_NAME>
```

Mode

SD-WAN Group

Description

Set SD-WAN group name.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

Example

```
name "VoIP"
```

Syntax

```
interface <SDWAN_GROUP_MEMBER>
```

Mode

SD-WAN Group

Description

Add/Edit group member.

Options

<SDWAN_GROUP_MEMBER> WAN interface name.
Example: *abc*

Example

```
interface X2
```

Syntax

```
no interface <SDWAN_CURRENT_GROUP_MEMBER>
```

Mode

SD-WAN Group

Description

Remove group member.

Options

<SDWAN_CURRENT_GROUP_MEMBER> Group Member Name.
Example: *abc*

Example

```
no interface X1
```

Syntax

```
no interfaces
```

Mode

SD-WAN Group

Description

Remove all group members.

Example

```
no interfaces
```

Syntax

```
priority <UINT8>
```

Mode

SD-WAN Group Member

Description

Member Priority in the group.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
priority 2
```

Syntax

```
path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN

Description

Add/edit SD-WAN path selection profile.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
path-selection-profile "VoIP"
```

Syntax

```
no path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN

Description

Delete a SD-WAN path selection profile.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no path-selection-profile "Best of All"
```

Syntax

```
no path-selection-profiles
```

Mode

SD-WAN

Description

Delete all SD-WAN path selection profiles.

Example

```
no path-selection-profiles
```

Syntax

```
name <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SD-WAN Path Selection Profile name.

Options

<SDWAN_PATH_SELECTION_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Best of All"
```

Syntax

```
sdwan-group <SDWAN_PATH_SELECTION_PROFILE_GROUP_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SD-WAN group.

Options

<SDWAN_PATH_SELECTION_PROFILE_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
sdwan-group "Interface Group 1"
```

Syntax

```
no sdwan-group
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear SD-WAN group.

Example

```
no sdwan-group
```

Syntax

```
sla-probe <SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_PROBE_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SLA probe.

Options

<SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_PROBE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
sla-probe "Ping Probe"
```

Syntax

```
no sla-probe
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear SLA probe.

Example

```
no sla-probe
```

Syntax

```
sla-class <SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_CLASS_NAME>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set SLA class.

Options

<SDWAN_PATH_SELECTION_PROFILE_PERFORMANCE_CLASS_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
sla-class "Lowest Jitter"
```

Syntax

```
no sla-class
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear SLA class.

Example

```
no sla-class
```

Syntax

```
backup-interface <SDWAN_PATH_SELECTION_PROFILE_BACKUP_INTERFACE>
```

Mode

SD-WAN Path Selection Profiles.

Description

Set backup interface.

Options

<SDWAN_PATH_SELECTION_PROFILE_BACKUP_INTERFACE> Backup interface name.
Example: *X0*

Example

```
backup-interface X5
```

Syntax

```
no backup-interface
```

Mode

SD-WAN Path Selection Profiles.

Description

Clear backup interface.

Example

```
no backup-interface
```

Syntax

```
probe-default-up
```

Mode

SD-WAN Path Selection Profiles.

Description

Enable SLA probe default state is UP.

Example

```
probe-default-up
```

Syntax

```
no probe-default-up
```

Mode

SD-WAN Path Selection Profiles.

Description

Disable SLA probe default state is UP.

Example

```
no probe-default-up
```

Syntax

```
reset-connections
```

Mode

SD-WAN Path Selection Profiles.

Description

Enable reset connections if path does not meet the performance criteria.

Example

```
reset-connections
```

Syntax

```
no reset-connections
```

Mode

SD-WAN Path Selection Profiles.

Description

Disable reset connections if path does not meet the performance criteria.

Example

```
no reset-connections
```

Syntax

show sdwan sla-class-objects

Mode

All Modes

Description

Show all SD-WAN SLA Class Objects.

Example

show sdwan sla-class-objects

Syntax

show sdwan sla-class-object <SDWAN_SLA_CLASS_OBJECT_NAME>

Mode

All Modes

Description

Show SD-WAN SLA Class Object.

Options

<SDWAN_SLA_CLASS_OBJECT_NAME> Atom Object name.
Example: *Lowest Jitter*

Example

show sdwan sla-class-object "Best of All"

Syntax

show sdwan sla-probes [{ pending-config | with-pending-config } | status]

Mode

All Modes

Description

Show all SD-WAN SLA Probes.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show all SD-WAN SLA Probes status.

Example

show sdwan-probe sla-probes

Syntax

```
show sdwan sla-probe <SDWAN_PROBE_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN SLA Probe.

Options

<SDWAN_PROBE_NAME> Atom Object name.
Example: *Web Services Monitor*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show a specific SD-WAN SLA Probe status.

Example

```
show sdwan-probe sla-probe "Remote Servers"
```

Syntax

```
show sdwan group <SDWAN_GROUP_NAME> [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN configuration or status.

Options

<SDWAN_GROUP_NAME> SD-WAN Group Name.
Example: *Social Networking*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

status Show SD-WAN group status.

Example

```
show sdwan group "WAN Group"
```

Syntax

```
show sdwan groups [ { pending-config | with-pending-config } | status ]
```

Mode

All Modes

Description

Show SD-WAN configuration or status.

Options

<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.
<i>status</i>	Show SD-WAN groups status.

Example

```
show sdwan groups
```

Syntax

```
show sdwan path-selection-profiles
```

Mode

All Modes

Description

Show all SD-WAN path selection profiles.

Example

```
show sdwan path-selection-profiles
```

Syntax

```
show sdwan path-selection-profile <SDWAN_PATH_SELECTION_PROFILE_NAME>
```

Mode

All Modes

Description

Show SD-WAN path selection profile.

Options

<i><SDWAN_PATH_SELECTION_PROFILE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
show sdwan path-selection-profile "Best of All"
```

Syntax

```
no security-action-profile [ uuid ] <SECURITY_ACTION_PROFILE_NAME>
```

Mode

Config

Description

Delete security action profile.

Options

<i>uuid</i>	Delete a security action profile by UUID.
<i><SECURITY_ACTION_PROFILE_NAME></i>	Security action profile name. Example: <i>MySecurityActionProfile</i>

Example

```
no security-action-profile "Office Security Action Profile"
```

Syntax

no security-action-profiles

Mode

Config

Description

Delete all security action profiles.

Example

no security-action-profiles

Syntax

security-action-profile [uuid] <SECURITY_ACTION_PROFILE_NAME>

Mode

Config

Description

Add/Edit security action profile and enter configuration mode.

Options

<i>uuid</i>	Edit security action profile by UUID.
<i><SECURITY_ACTION_PROFILE_NAME></i>	Security action profile name. Example: <i>MySecurityActionProfile</i>

Example

security-action-profile "Office Security Action Profile"

Syntax

clone security-action-profile [uuid] <SECURITY_ACTION_PROFILE_NAME> [new-name <WORD>]

Mode

Config

Description

Clone security action profile.

Options

<i>uuid</i>	Edit security action profile by UUID.
<i><SECURITY_ACTION_PROFILE_NAME></i>	Security action profile name. Example: <i>MySecurityActionProfile</i>
<i>new-name</i>	Clone a security action profile with a new name.
<i><WORD></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

clone security-action-profile "Office Security Action Profile"

Syntax

uuid <UUID>

Mode

Security Action Profile

Description

Set security action profile UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Security Action Profile

Description

Clear security action profile UUID.

Example

no uuid

Syntax

name <SECURITY_ACTION_PROFILE_NAME>

Mode

Security Action Profile

Description

Security action profile name.

Options

<SECURITY_ACTION_PROFILE_NAME> Security action profile name.
Example: *MySecurityActionProfile*

Example

name "Office Security Action Profile"

Syntax

no name

Mode

Security Action Profile

Description

Clear security action profile name.

Example

no name

Syntax

bandwidth-management

Mode

Security Action Profile

Description

Enter ethernet bandwidth management configuration mode.

Example

bandwidth-management

Syntax

aggregation-method { per-action | per-policy }

Mode

Bandwidth Management

Description

Set bandwidth method.

Options

per-action Set bandwidth method to per action.

per-policy Set bandwidth method to per policy.

Example

aggregation-method per-action

Syntax

egress enable

Mode

Bandwidth Management

Description

Enable egress bandwidth management.

Example

egress enable

Syntax

no egress enable

Mode

Bandwidth Management

Description

Disable egress bandwidth management.

Example

```
no egress enable
```

Syntax

```
egress bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Bandwidth Management

Description

Set Bandwidth object.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\ "Corp High Priority" \`

Example

```
egress bandwidth-object "Corp Access Bandwidth Object"
```

Syntax

```
no egress bandwidth-object
```

Mode

Bandwidth Management

Description

Clear Bandwidth object.

Example

```
no egress bandwidth-object
```

Syntax

```
ingress enable
```

Mode

Bandwidth Management

Description

Enable ingress bandwidth management.

Example

```
ingress enable
```

Syntax

```
no ingress enable
```

Mode

Bandwidth Management

Description

Disable ingress bandwidth management.

Example

```
no ingress enable
```

Syntax

```
ingress bandwidth-object <BANDWIDTH_RULE_NAME>
```

Mode

Bandwidth Management

Description

Enable ingress bandwidth management and configure.

Options

<BANDWIDTH_RULE_NAME> Bandwidth object name.
Example: `\ "Corp High Priority" \`

Example

```
ingress bandwidth-object "Corp Access Bandwidth Object"
```

Syntax

```
no ingress bandwidth-object
```

Mode

Bandwidth Management

Description

Disable ingress bandwidth management.

Example

```
no ingress bandwidth-object
```

Syntax

```
usage-tracking
```

Mode

Bandwidth Management

Description

Enable tracking bandwidth usage.

Example

```
usage-tracking
```

Syntax

```
no usage-tracking
```

Mode

Bandwidth Management

Description

Disable tracking bandwidth usage.

Example

no usage-tracking

Syntax

quality-of-service class-of-service { explicit { { background | best-effort | controlled-load | excellent-effort | network-control | spare | video | voice } } | map | preserve }

Mode

Security Action Profile

Description

Set 802.1p marking action.

Options

<i>explicit</i>	Set explicit marking.
<i>background</i>	Background.
<i>best-effort</i>	Best effort.
<i>controlled-load</i>	Controlled load.
<i>excellent-effort</i>	Excellent effort.
<i>network-control</i>	Network control.
<i>spare</i>	Spare.
<i>video</i>	Video (<100ms latency).
<i>voice</i>	Voice (<10ms latency).
<i>map</i>	Map marking.
<i>preserve</i>	Preserve marking.

Example

quality-of-service class-of-service preserve

Syntax

cos-override

Mode

Security Action Profile

Description

Allow 802.1p marking to override DSCP values.

Example

cos-override

Syntax

no cos-override

Mode

Security Action Profile

Description

Disable allowing 802.1p marking to override DSCP values.

Example

no cos-override

Syntax

no quality-of-service { class-of-service | dscp }

Mode

Security Action Profile

Description

Clear DSCP and 802.1p marking settings.

Options

class-of-service No 802.1p tagging.

dscp Clear DSCP values.

Example

no quality-of-service dscp

Syntax

quality-of-service dscp { explicit <UINT8> | map | preserve }

Mode

Security Action Profile

Description

Set DSCP marking action.

Options

explicit Set explicit marking.

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

map Map marking.

preserve Preserve marking.

Example

quality-of-service dscp preserve

Syntax

gateway-antivirus

Mode

Security Action Profile

Description

Enter security policy gateway anti-Virus configuration mode.

Example

gateway-antivirus

Syntax

enable

Mode

Gateway Anti-Virus

Description

Enable gateway anti-virus.

Example

enable

Syntax

no enable

Mode

Gateway Anti-Virus

Description

Disable gateway anti-virus.

Example

no enable

Syntax

cloud

Mode

Gateway Anti-Virus

Description

Enable cloud gateway anti-virus database.

Example

cloud

Syntax

no cloud

Mode

Gateway Anti-Virus

Description

Disable cloud gateway anti-virus database.

Example

```
no cloud
```

Syntax

```
inbound
```

Mode

Gateway Anti-Virus

Description

Enable inbound inspection.

Example

```
inbound
```

Syntax

```
no inbound
```

Mode

Gateway Anti-Virus

Description

Disable inbound inspection.

Example

```
no inbound
```

Syntax

```
outbound
```

Mode

Gateway Anti-Virus

Description

Enable outbound inspection.

Example

```
outbound
```

Syntax

```
no outbound
```

Mode

Gateway Anti-Virus

Description

Disable outbound inspection.

Example

```
no outbound
```

Syntax

```
prevent
```

Mode

Gateway Anti-Virus

Description

Disable prevention.

Example

```
prevent
```

Syntax

```
no prevent
```

Mode

Gateway Anti-Virus

Description

Enable prevention.

Example

```
no prevent
```

Syntax

```
packet-monitor
```

Mode

Gateway Anti-Virus

Description

Enable packet monitor.

Example

```
packet-monitor
```

Syntax

```
no packet-monitor
```

Mode

Gateway Anti-Virus

Description

Disable packet monitor.

Example

no packet-monitor

Syntax

log

Mode

Gateway Anti-Virus

Description

Enable log.

Example

log

Syntax

no log

Mode

Gateway Anti-Virus

Description

Disable log.

Example

no log

Syntax

password-protected-zip

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of password-protected ZIP files.

Example

password-protected-zip

Syntax

no password-protected-zip

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of password-protected ZIP files for the specified protocols.

Example

no password-protected-zip

Syntax

ms-office-macros

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of MS-Office type files containing macros (VBA 5 and above).

Example

ms-office-macros

Syntax

no ms-office-macros

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of MS-Office type files containing macros (VBA 5 and above) for the specified protocols.

Example

no ms-office-macros

Syntax

packed-executables

Mode

Gateway Anti-Virus

Description

Disable restricting transfer of packed executable files (UPX, FSG, etc.).

Example

restrict packed-executables http

Syntax

no packed-executables

Mode

Gateway Anti-Virus

Description

Enable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Example

no packed-executables http

Syntax

smtp-responses

Mode

Gateway Anti-Virus

Description

Enable SMTP responses.

Example

smtp-responses

Syntax

no smtp-responses

Mode

Gateway Anti-Virus

Description

Disable SMTP responses.

Example

no smtp-responses

Syntax

eicar-detection

Mode

Gateway Anti-Virus

Description

Enable detection of EICAR test virus.

Example

eicar-detection

Syntax

no eicar-detection

Mode

Gateway Anti-Virus

Description

Disable detection of EICAR test virus.

Example

no eicar-detection

Syntax

http-byte-range

Mode

Gateway Anti-Virus

Description

Enable HTTP Byte-Range requests with Gateway AV.

Example

```
http-byte-range
```

Syntax

```
no http-byte-range
```

Mode

Gateway Anti-Virus

Description

Disable HTTP Byte-Range requests with Gateway AV.

Example

```
no http-byte-range
```

Syntax

```
ftp-rest
```

Mode

Gateway Anti-Virus

Description

Enable FTP 'REST' requests with Gateway AV.

Example

```
ftp-rest
```

Syntax

```
no ftp-rest
```

Mode

Gateway Anti-Virus

Description

Disable FTP 'REST' requests with Gateway AV.

Example

```
no ftp-rest
```

Syntax

```
scan-high-compression
```

Mode

Gateway Anti-Virus

Description

Scan parts of files with high compression ratios.

Example

```
scan-high-compression
```

Syntax

```
no scan-high-compression
```

Mode

Gateway Anti-Virus

Description

Do not scan parts of files with high compression ratios.

Example

```
no scan-high-compression
```

Syntax

```
threat
```

Mode

Security Action Profile

Description

Enter security policy threat configuration mode.

Example

```
threat
```

Syntax

```
enable
```

Mode

Threat Prevention

Description

Enable threat prevention.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Threat Prevention

Description

Disable threat prevention.

Example

```
no enable
```

Syntax

```
based-on { global | profile }
```

Mode

Threat Prevention

Description

Set what threat profile is based on.

Options

global Global settings.

profile Profile settings.

Example

```
based-on profile
```

Syntax

```
prevent enable
```

Mode

Threat Prevention

Description

Enable prevent.

Example

```
prevent enable
```

Syntax

```
no prevent enable
```

Mode

Threat Prevention

Description

Disable prevent.

Example

```
no prevent enable
```

Syntax

```
prevent profile { all | group <THREAT_PROFILE_NAME> }
```

Mode

Threat Prevention

Description

Assign threat object group to threat profile prevention.

Options

<i>all</i>	Assign all to threat profile prevention.
<i>group</i>	Threat object group.
<i><THREAT_PROFILE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>DNS Category Profile</i>

Example

prevent profile group "Corp Access Threat Group"

Syntax

packet-monitor enable

Mode

Threat Prevention

Description

Enable threat profile packet monitor.

Example

packet-monitor enable

Syntax

no packet-monitor enable

Mode

Threat Prevention

Description

Disable threat profile packet monitor.

Example

no packet-monitor enable

Syntax

packet-monitor profile { all | group <THREAT_PROFILE_NAME> }

Mode

Threat Prevention

Description

Assign threat object group to threat profile packet monitor.

Options

<i>all</i>	Assign all to threat profile packet monitor.
<i>group</i>	Threat object group.
<i><THREAT_PROFILE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\".

Example

packet-monitor profile group "Corp Access Threat Group"

Syntax

log enable

Mode

Threat Prevention

Description

Enable threat profile log.

Example

log enable

Syntax

no log enable

Mode

Threat Prevention

Description

Disable threat profile log.

Example

no log enable

Syntax

log profile { all | group <THREAT_PROFILE_NAME> }

Mode

Threat Prevention

Description

Assign threat object group to threat profile log.

Options

all	Assign all to threat profile log.
group	Threat object group.
<THREAT_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>DNS Category Profile</i>

Example

log profile group "Corp Access Threat Group"

Syntax

log redundancy <UINT32>

Mode

Threat Prevention

Description

Set the log redundancy filter interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

log redundancy 3

Syntax

no log redundancy

Mode

Threat Prevention

Description

Clear the log redundancy filter interval.

Example

no log redundancy

Syntax

signature-group high-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }

Mode

Threat Prevention

Description

Enable signature group high priority detection and log redundancy.

Options

- log-all*** Log all.
- log-redundancy <UINT32>*** Set log redundancy in seconds.
Integer in the form: D OR 0xHHHHHHHH.
Example: *123*
- packet-monitor-all*** Packet monitor all.
- prevent-all*** Prevent all.

Example

signature-group high-priority prevent-all
signature-group high-priority log-redundancy 60

Syntax

signature-group medium-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }

Mode

Threat Prevention

Description

Enable signature group medium priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i> <i><UINT32></i>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
signature-group medium-priority prevent-all
signature-group medium-priority log-redundancy 60
```

Syntax

```
signature-group low-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Threat Prevention

Description

Enable signature group low priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i> <i><UINT32></i>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
signature-group low-priority prevent-all
signature-group low-priority log-redundancy 60
```

Syntax

```
no signature-group high-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Threat Prevention

Description

Disable signature group high priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no signature-group high-priority prevent-all
no signature-group high-priority log-redundancy
```

Syntax

```
no signature-group medium-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Threat Prevention

Description

Disable signature group medium priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no signature-group medium-priority prevent-all
no signature-group medium-priority log-redundancy
```

Syntax

```
no signature-group low-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Threat Prevention

Description

Disable signature group low priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no signature-group low-priority prevent-all
no signature-group low-priority log-redundancy
```

Syntax

anti-spyware

Mode

Security Action Profile

Description

Enter security policy anti-spyware configuration mode.

Example

anti-spyware

Syntax

enable

Mode

Anti-Spyware

Description

Enable anti-spyware prevention.

Example

enable

Syntax

no enable

Mode

Anti-Spyware

Description

Disable anti-spyware prevention.

Example

no enable

Syntax

inbound

Mode

Anti-Spyware

Description

Enable inbound inspection.

Example

inbound

Syntax

no inbound

Mode

Anti-Spyware

Description

Disable inbound inspection.

Example

no inbound

Syntax

outbound

Mode

Anti-Spyware

Description

Enable outbound inspection.

Example

outbound

Syntax

no outbound

Mode

Anti-Spyware

Description

Disable outbound inspection.

Example

no outbound

Syntax

smtp-responses

Mode

Anti-Spyware

Description

Enable SMTP responses.

Example

smtp-responses

Syntax

no smtp-responses

Mode

Anti-Spyware

Description

Disable SMTP responses.

Example

no smtp-responses

Syntax

http-clientless-notification

Mode

Anti-Spyware

Description

Enable anti-spyware http clientless notification.

Example

http-clientless-notification

Syntax

no http-clientless-notification

Mode

Anti-Spyware

Description

Disable anti-spyware http clientless notification.

Example

no http-clientless-notification

Syntax

signature-group high-priority { log | log-redundancy <UINT32> | packet-monitor | prevent }

Mode

Anti-Spyware

Description

Enable signature group high priority detection and log redundancy.

Options

<i>log</i>	Log all.
<i>log-redundancy</i> <i><UINT32></i>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
<i>packet-monitor</i>	Packet monitor all.
<i>prevent</i>	Prevent all.

Example

```
signature-group high-priority prevent
signature-group high-priority log-redundancy 60
```

Syntax

```
signature-group medium-priority { log | log-redundancy <UINT32> | packet-monitor | prevent }
```

Mode

Anti-Spyware

Description

Enable signature group medium priority detection and log redundancy.

Options

log	Log all.
log-redundancy	Set log redundancy in seconds.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
packet-monitor	Packet monitor all.
prevent	Prevent all.

Example

```
signature-group medium-priority prevent
signature-group medium-priority log-redundancy 60
```

Syntax

```
signature-group low-priority { log | log-redundancy <UINT32> | packet-monitor | prevent }
```

Mode

Anti-Spyware

Description

Enable signature group low priority detection and log redundancy.

Options

log	Log all.
log-redundancy	Set log redundancy in seconds.
<UINT32>	Integer in the form: D OR 0xHHHHHHHH. Example: 123
packet-monitor	Packet monitor all.
prevent	Prevent all.

Example

```
signature-group low-priority prevent
signature-group low-priority log-redundancy 60
```

Syntax

```
no signature-group high-priority { log | log-redundancy | packet-monitor | prevent }
```

Mode

Anti-Spyware

Description

Disable signature group high priority detection and log redundancy.

Options

<i>log</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor</i>	Packet monitor all.
<i>prevent</i>	Prevent all.

Example

```
no signature-group high-priority prevent
no signature-group high-priority log-redundancy
```

Syntax

```
no signature-group medium-priority { log | log-redundancy | packet-monitor | prevent }
```

Mode

Anti-Spyware

Description

Disable signature group medium priority detection and log redundancy.

Options

<i>log</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor</i>	Packet monitor all.
<i>prevent</i>	Prevent all.

Example

```
no signature-group medium-priority prevent
no signature-group medium-priority log-redundancy
```

Syntax

```
no signature-group low-priority { log | log-redundancy | packet-monitor | prevent }
```

Mode

Anti-Spyware

Description

Disable signature group low priority detection and log redundancy.

Options

<i>log</i>	Log all.

log-redundancy Clear log redundancy.

packet-monitor Packet monitor all.

prevent Prevent all.

Example

```
no signature-group low-priority prevent
no signature-group low-priority log-redundancy
```

Syntax

```
botnet
```

Mode

Security Action Profile

Description

Enter security policy botnet configuration mode.

Example

```
botnet
```

Syntax

```
enable
```

Mode

Botnet

Description

Enable botnet filter.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Botnet

Description

Disable botnet filter.

Example

```
no enable
```

Syntax

```
packet-monitor
```

Mode

Botnet

Description

Enable botnet filter packet monitor.

Example

packet-monitor

Syntax

no packet-monitor

Mode

Botnet

Description

Disable botnet filter packet monitor.

Example

no packet-monitor

Syntax

log enable

Mode

Botnet

Description

Enable botnet filter log.

Example

log enable

Syntax

no log enable

Mode

Botnet

Description

Disable botnet filter log.

Example

no log enable

Syntax

log redundancy <UINT32>

Mode

Botnet

Description

Set redundancy filter interval.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

log redundancy 1

Syntax

no log redundancy

Mode

Botnet

Description

Disable botnet filter log.

Example

no log redundancy

Syntax

content-filter

Mode

Security Action Profile

Description

Enter security policy content filter configuration mode.

Example

content-filter

Syntax

enable

Mode

Content Filter

Description

Enable content filtering.

Example

enable

Syntax

no enable

Mode

Content Filter

Description

Disable content filtering.

Example

```
no enable
```

Syntax

```
action { allow | confirm | passphrase }
```

Mode

Content Filter

Description

Set content filter action.

Options

allow Allow.

confirm Confirm.

passphrase Passphrase.

Example

```
action confirm
```

Syntax

```
safe-search
```

Mode

Content Filter

Description

Enable safe search enforcement.

Example

```
safe-search
```

Syntax

```
no safe-search
```

Mode

Content Filter

Description

Disable safe search enforcement.

Example

```
no safe-search
```

Syntax

google-force-safe-search

Mode

Content Filter

Description

Enable Google force safe search.

Example

google-force-safe-search

Syntax

no google-force-safe-search

Mode

Content Filter

Description

Disable Google force safe search.

Example

no google-force-safe-search

Syntax

youtube-restrict-mode

Mode

Content Filter

Description

Enable YouTube restrict mode.

Example

youtube-restrict-mode

Syntax

no youtube-restrict-mode

Mode

Content Filter

Description

Disable YouTube restrict mode.

Example

no youtube-restrict-mode

Syntax

bing-force-safe-search

Mode

Content Filter

Description

Enable Bing force safe search.

Example

bing-force-safe-search

Syntax

no bing-force-safe-search

Mode

Content Filter

Description

Disable Bing force safe search.

Example

no bing-force-safe-search

Syntax

wipe-cookies

Mode

Content Filter

Description

Enable wipe cookies.

Example

wipe-cookies

Syntax

no wipe-cookies

Mode

Content Filter

Description

Disable wipe cookies.

Example

no wipe-cookies

Syntax

flow-reporting

Mode

Content Filter

Description

Enable flow reporting.

Example

flow-reporting

Syntax

no flow-reporting

Mode

Content Filter

Description

Disable flow reporting.

Example

no flow-reporting

Syntax

passphrase page { custom <WORD> | default }

Mode

Content Filter

Description

Set passphrase page.

Options

- custom** Use custom defined page.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default** Use default page.

Example

passphrase page custom "<html> ... </html>"
passphrase page default

Syntax

no passphrase page

Mode

Content Filter

Description

Clear passphrase page.

Example

no passphrase page

Syntax

passphrase password <ENC_PASSWORD>

Mode

Content Filter

Description

Set passphrase password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

passphrase password 123456

Syntax

no passphrase password

Mode

Content Filter

Description

Clear passphrase password.

Example

no passphrase password

Syntax

passphrase active-time <UINT32>

Mode

Content Filter

Description

Set passphrase active time.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

passphrase active-time 60

Syntax

confirm page { custom <WORD> | default }

Mode

Content Filter

Description

Set confirm page.

Options

- custom**

Use custom defined page.
- <WORD>**

Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- default**

Use default page.

Example

```
confirm page custom "<html> ... </html>"
confirm page default
```

Syntax

```
no confirm page
```

Mode

Content Filter

Description

Clear confirm page.

Example

```
no confirm page
```

Syntax

```
confirm active-time <UINT32>
```

Mode

Content Filter

Description

Set confirm active time.

Options

- <UINT32>**

Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
confirm active-time 60
```

Syntax

```
consent required
```

Mode

Content Filter

Description

Enable consent.

Example

```
consent required
```

Syntax

no consent required

Mode

Content Filter

Description

Disable consent.

Example

no consent required

Syntax

consent user-idle-timeout <UINT32>

Mode

Content Filter

Description

Set consent user idle timeout.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

consent user-idle-timeout 15

Syntax

consent optional page-url <WORD>

Mode

Content Filter

Description

Set consent optional page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

consent optional page-url 1.1.1.1/consentOptional.html

Syntax

no consent optional page-url

Mode

Content Filter

Description

Clear consent optional page URL.

Example

no consent optional page-url

Syntax

consent mandatory page-url <WORD>

Mode

Content Filter

Description

Set consent mandatory page URL.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

consent mandatory page-url 1.1.1.1/consentMandatory.html

Syntax

no consent mandatory page-url

Mode

Content Filter

Description

Clear consent mandatory page URL.

Example

no consent mandatory page-url

Syntax

consent mandatory address { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } | any | group <ADDR_HNR_GROUP_MIXED> | name <ADDR_HNR_NAME_MIXED> }

Mode

Content Filter

Description

Set consent mandatory filtering address.

Options

ipv6	IPv6 Address object.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\nExample: IPV4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n

Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

<i>range</i>	Specify IP range.
<ADDR_BEGIN>	IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH.HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
<i>any</i>	All address.
<i>group</i>	Address object group name.
<ADDR_HNR_GROUP_MIXED>	Host/network/range group address object name. Example: <i>Sales & Marketing Network Access Points</i>
<i>name</i>	Address object name.
<ADDR_HNR_NAME_MIXED>	Host/network/range address object name. Example: <i>Web Server</i>

Example

```
consent mandatory address host 192.168.168.168
consent mandatory address network 192.168.168.0 255.255.255.0
consent mandatory address range 192.168.168.1 192.168.168.10
consent mandatory address ipv6 host fec0:1:1
consent mandatory address ipv6 network fec0:1: 64
consent mandatory address ipv6 range fec0:1:1 fec0:1:100
consent mandatory address any
consent mandatory address group "Consent Mandatory Address Group"
consent mandatory address name "Consent Mandatory Address Object"
```

Syntax

no consent mandatory address

Mode

Content Filter

Description

Clear consent mandatory filtering address.

Example

no consent mandatory address

Syntax

custom-header insertion

Mode

Content Filter

Description

Enable custom header insertion.

Example

custom-header insertion

Syntax

no custom-header insertion

Mode

Description

Disable custom header insertion.

Example

```
no custom-header insertion
```

Syntax

```
custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter

Description

Add new custom header entry into custom header list.

Options

- <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> Content filter custom header domain.
Example: \ "YouTube.com" \ "
- <CONTENT_FILTER_CUSTOM_HEADER_KEY> Content filter custom header key.
Example: \ "YouTube-Restrict-Mode" \ "
- <CONTENT_FILTER_CUSTOM_HEADER_VALUE> Content filter custom header value.
Example: \ "Strict" \ "

Example

```
custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

```
no custom-header entry <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> <CONTENT_FILTER_CUSTOM_HEADER_KEY>
<CONTENT_FILTER_CUSTOM_HEADER_VALUE>
```

Mode

Content Filter

Description

Delete custom header entry from custom header list.

Options

- <CONTENT_FILTER_CUSTOM_HEADER_DOMAIN> Content filter custom header domain.
Example: \ "YouTube.com" \ "
- <CONTENT_FILTER_CUSTOM_HEADER_KEY> Content filter custom header key.
Example: \ "YouTube-Restrict-Mode" \ "
- <CONTENT_FILTER_CUSTOM_HEADER_VALUE> Content filter custom header value.
Example: \ "Strict" \ "

Example

```
no custom-header entry "YouTube.com" "YouTube-Restrict-Mode" "Strict"
```

Syntax

```
no custom-header entries
```

Mode

Content Filter
Security Action Profile

Description

Remove all custom header entries from custom header list.

Example

no custom-header entries

Syntax

reporting

Mode

Security Action Profile

Description

Enter security policy reporting configuration mode.

Example

reporting

Syntax

profile { default | global | name <REPORTING_PROFILE_NAME> }

Mode

Reporting

Description

Assign reporting profile object to action profile.

Options

<i>default</i>	Default reporting profile.
<i>global</i>	Global reporting profile name.
<i>name</i>	Reporting profile name.
<i><REPORTING_PROFILE_NAME></i>	Reporting profile name. Example: <i>MyReportingProfile</i>

Example

profile name "Corp Reporting Policy"

Syntax

packet-monitor

Mode

Reporting

Description

Enable packet monitor.

Example

packet-monitor

Syntax

no packet-monitor

Mode

Reporting

Description

Disable packet monitor.

Example

no packet-monitor

Syntax

user-actions

Mode

Security Action Profile

Description

Enter security policy user actions configuration mode.

Example

user-actions

Syntax

block-page dropped-connections

Mode

User Actions

Description

Enable show block page for dropped client web connections.

Example

block-page dropped-connections

Syntax

no block-page dropped-connections

Mode

User Actions

Description

Disable show block page for dropped client web connections.

Example

no block-page dropped-connections

Syntax

block-details

Mode

User Actions

Description

Enable include policy block details.

Example

block-details

Syntax

no block-details

Mode

User Actions

Description

Disable show block page for dropped client web connections.

Example

no block-details

Syntax

block-page object { default | global | name <BLOCK_PAGE_NAME> }

Mode

User Actions

Description

Assign block page object to action profile.

Options

<i>default</i>	Default.
<i>global</i>	Global.
<i>name</i>	Block page object name.
<i><BLOCK_PAGE_NAME></i>	Block page name. Example: <i>\ "Corp Block Page\ "</i>

Example

block-page object global

Syntax

bypass-sso

Mode

User Actions

Description

Enable bypassing SSO for connections that match the policy.

Example

Syntax

no bypass-ss0

Mode

User Actions

Description

Disable bypassing SSO for connections that match the policy.

Example

no bypass-ss0

Syntax

tcp timeout <UINT32>

Mode

Security Action Profile

Description

Set the TCP connection inactivity timeout (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

tcp timeout 15

Syntax

udp timeout <UINT32>

Mode

Security Action Profile

Description

Set the UPD connection inactivity timeout (seconds).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

udp timeout 30

Syntax

fragments

Mode

Security Action Profile

Description

Allow fragmented packets on this access rule.

Example

```
fragments
```

Syntax

```
no fragments
```

Mode

Security Action Profile

Description

Disable fragmented packets on this access rule.

Example

```
no fragments
```

Syntax

```
bypass-server-to-client-inspection
```

Mode

Security Action Profile

Description

Enable bypass inspection of server to client packets.

Example

```
bypass-server-to-client-inspection
```

Syntax

```
no bypass-server-to-client-inspection
```

Mode

Security Action Profile

Description

Disable bypass inspection of server to client packets.

Example

```
no bypass-server-to-client-inspection
```

Syntax

```
sip
```

Mode

Security Action Profile

Description

Enable SIP transformations.

Example

```
sip
```

Syntax

```
no sip
```

Mode

Security Action Profile

Description

Disble SIP transformations.

Example

```
no sip
```

Syntax

```
h323
```

Mode

Security Action Profile

Description

Enable H.323 transformations.

Example

```
h323
```

Syntax

```
no h323
```

Mode

Security Action Profile

Description

Disble H.323 transformations.

Example

```
no h323
```

Syntax

```
unauthenticated-redirect
```

Mode

Security Action Profile

Description

Disable don't redirect unauthenticated users to log in.

Example

unauthenticated-redirect

Syntax

no unauthenticated-redirect

Mode

Security Action Profile

Description

Enable don't redirect unauthenticated users to log in.

Example

no unauthenticated-redirect

Syntax

no dos-policy uuid <DOS_POLICY_UUID>

Mode

Config

Description

Delete DoS policy by uuid.

Options

<DOS_POLICY_UUID> DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*

Example

no dos-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no dos-policies

Mode

Config

Description

Delete all DoS policies.

Example

no dos-policies

Syntax

dos-policy uuid <DOS_POLICY_UUID>

Mode

Config

Description

Add/Edit DoS policy and enter configuration mode.

Options

<DOS_POLICY_UUID> DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*

Example

dos-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

clone dos-policy uuid <DOS_POLICY_UUID> location { after | before }

Mode

Config

Description

Clone DoS policy.

Options

uuid Clone DoS policy by UUID.

<DOS_POLICY_UUID> DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*

location Location to clone Dos policy.

after Clone Dos policy after.

before Clone Dos policy before.

Example

clone dos-policy uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c location before

Syntax

clear dos-policy uuid <DOS_POLICY_UUID> statistics

Mode

Config

Description

Clear firewall DoS policy statistics by UUID.

Options

uuid UUID

<DOS_POLICY_UUID> DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*

statistics Clear firewall DoS policy statistics by UUID.

Example

clear dos-policy uuid 00000000-0000-0001-1e00-2cb8ed4acd38 statistics

Syntax

clear dos-policies statistics

Mode

Config

Description

Clear firewall DoS policies statistics.

Example

```
clear dos-policies statistics
```

Syntax

```
uuid <DOS_POLICY_UUID>
```

Mode

Dos Policy

Description

DoS policy UUID.

Options

<DOS_POLICY_UUID> DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*

Example

```
uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Dos Policy

Description

DoS policy UUID.

Example

```
no uuid
```

Syntax

```
name <DOS_POLICY_NAME>
```

Mode

Dos Policy

Description

DoS policy name.

Options

<DOS_POLICY_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Office DoS Policy"
```

Syntax

no name

Mode

Dos Policy

Description

Clear DoS policy name.

Example

no name

Syntax

```
priority { auto | end | manual <UINT32> }
```

Mode

Dos Policy

Description

Set Dos policy priority.

Options

<i>auto</i>	Set auto priority for DoS policy.
<i>end</i>	Insert the policy at the end.
<i>manual</i>	Set manual priority for DoS policy.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

```
priority auto
priority manual 2
```

Syntax

enable

Mode

Dos Policy

Description

Enable this DoS policy.

Example

enable

Syntax

no enable

Mode

Dos Policy

Description

Disable this DoS policy.

Example

no enable

Syntax

comment <WORD>

Mode

Dos Policy

Description

Specify a comment for this DoS policy.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

comment \"DoS for WAN access\"

Syntax

no comment

Mode

Dos Policy

Description

Clear a comment for this DoS policy.

Example

no comment

Syntax

destination address { { { [ipv6] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
| any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }

Mode

Dos Policy

Description

Specify a destination for this Dos policy.

Options

ipv6	IPv6 address object.
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: IPV4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n.

Example: *IPV4: 255.255.255.0\nIPV6: /64\n*

range	Address object range.
<ADDR_BEGIN>	IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_MIXED>	Group address object name. Example: <i>Sales Group</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_MIXED>	Address object name. Example: <i>Web Server</i>

Example

destination address name "Corporate Servers"

Syntax

```
source address { { { [ ipv6 ] { host <ADDR_HOST> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } } |  
any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> } }
```

Mode

Dos Policy

Description

Specify source address for this DoS policy.

Options

ipv6	IPv6 address object.
host	Address object host.
<ADDR_HOST>	IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
network	Address object network.
<ADDR_NETWORK>	IPV4: address object IPv4 network in the form: D.D.D.D\nIPV6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.168.0\nIPV6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPV4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPV6: address object IPv6 netmask in the form: /D\n. Example: <i>IPV4: 255.255.255.0\nIPV6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPV4: address object IPv4 starting range in the form: D.D.D.D\nIPV6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.100\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPV4: address object IPv4 ending range in the form: D.D.D.D\nIPV6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPV4: 192.168.1.150\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>
any	Any address.
fqdn	Address object full qualified domain name.

<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
mac <ADDR_MAC>	Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>

Example

```
source address name "Corporate IT Administration"
```

Syntax

```
ip-version { ipv4 | ipv6 | mixed }
```

Mode

Dos Policy

Description

Specify IP version for this DoS policy.

Options

- ipv4** IPv4.
- ipv6** IPv6.
- mixed** Mixed.

Example

```
ip-version ipv4
```

Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Dos Policy

Description

Specify a service for this DoS policy.

Options

- any** Any destination service.
- group** Service group name.
<SVC_GROUP_NAME> Service object group name.
Example: *VOIP*
- name** Service object name.
<SVC_NAME> Service object name.
Example: *HTTPS*
- protocol** Service object protocol.

<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
service "HTTP"
```

Syntax

```
schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } }
```

Mode

Dos Policy

Description

Specify a schedule for this DoS policy.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule name "DoS Schedule"
```

Syntax

```
action { { bypass | protect } }
```

Mode

Dos Policy

Description

Set the action for this DoS policy.

Options

<i>bypass</i>	Allow traffic matching the criteria.
<i>protect</i>	Protect against traffic matching the criteria.

Example

```
action protect
```

Syntax

```
action-profile <DOS_ACTION_PROFILE_NAME>
```

Mode

Dos Policy

Description

Assign DoS action profile.

Options

<DOS_ACTION_PROFILE_NAME> Dos action profile name.
Example: *Office DoS Action Profile*

Example

```
action-profile "Corp DoS Profile"
```

Syntax

```
ticket tag1 <WORD>
```

Mode

Dos Policy

Description

Set Dos policy ticket tag.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag1 "Tag number 1"
```

Syntax

```
no ticket tag1
```

Mode

Dos Policy

Description

Clear Dos policy ticket tag1.

Example

```
no ticket tag1
```

Syntax

```
ticket tag2 <WORD>
```

Mode

Dos Policy

Description

Set Dos policy ticket tag.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag2 "Tag number 2"
```

Syntax

```
no ticket tag2
```

Mode

Dos Policy

Description

Clear Dos policy ticket tag2.

Example

```
no ticket tag2
```

Syntax

```
ticket tag3 <WORD>
```

Mode

Dos Policy

Description

Set Dos policy ticket tag.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag3 "Tag number 3"
```

Syntax

```
no ticket tag3
```

Mode

Dos Policy

Description

Clear Dos policy ticket tag3.

Example

```
no ticket tag3
```

Syntax

```
no website-objects
```

Mode

Config

Description

Delete all website objects.

Example

no website-objects

Syntax

no website-groups

Mode

Config

Description

Delete all website groups.

Example

no website-groups

Syntax

no website-object [uuid] <WEB_SITE_OBJ_NAME>

Mode

Config

Description

Delete a website object.

Options

- uuid** Select website object by UUID.
- <WEB_SITE_OBJ_NAME>** Website object name.
Example: *Website domain object*

Example

no website-object "webSiteObjName"

Syntax

no website-group [uuid] <WEB_SITE_GRP_NAME>

Mode

Config

Description

Delete a website group.

Options

- uuid** Select website group by UUID.
- <WEB_SITE_GRP_NAME>** Website group name.
Example: *Website domain group*

Example

```
no website-group "webSiteGrpName"
```

Syntax

```
website-object [ uuid ] <WEB_SITE_OBJ_NAME>
```

Mode

Config

Description

Add/Edit website object and enter configuration mode.

Options

- uuid** Select website object by UUID.
- <WEB_SITE_OBJ_NAME>** Website object name.
Example: *Website domain object*

Example

```
website-object "Website Object Name"
```

Syntax

```
clone website-object [ uuid ] <WEB_SITE_OBJ_NAME> [ new-name <WORD> ]
```

Mode

Config

Description

Clone website object.

Options

- uuid** Clone a website object by UUID.
- <WEB_SITE_OBJ_NAME>** Website object name.
Example: *Website domain object*
- new-name** Clone a website object with a new name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
clone website-object "Website Object Name"
```

Syntax

```
name <WEB_SITE_OBJ_NAME>
```

Mode

Website Object

Description

Set website object name.

Options

- <WEB_SITE_OBJ_NAME>** Website object name.
Example: *Website domain object*

Example

```
name "default website name"
```

Syntax

domain <WORD>

Mode

Website Object

Description

Add domain into website object.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

domain yahoo.com,google.com

Syntax

no domain

Mode

Website Object

Description

Remove domain from website object.

Example

no domain

Syntax

uuid <UUID>

Mode

Website Object

Description

Set website object UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Description

Clear website object UUID.

Example

no uuid

Syntax

website-group [uuid] <WEB_SITE_GRP_NAME>

Mode

Config

Description

Add/Edit website group and enter configuration mode.

Options

- uuid** Select website group by UUID.
- <WEB_SITE_GRP_NAME>** Website group name.
Example: *Website domain group*

Example

website-group "Web Site Group Name"

Syntax

clone website-group [uuid] <WEB_SITE_GRP_NAME> [new-name <WORD>]

Mode

Config

Description

Clone website group.

Options

- uuid** Clone a website group by UUID.
- <WEB_SITE_GRP_NAME>** Website group name.
Example: *Website domain group*
- new-name** Clone a website group with a new name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

clone website-group "Website Group Name"

Syntax

name <WEB_SITE_GRP_NAME>

Mode

Website Group

Description

Set website group name.

Options

<WEB_SITE_GRP_NAME> Website group name.
Example: *Website domain group*

Example

```
name "default group name"
```

Syntax

```
website-object <WEB_SITE_OBJ_NAME>
```

Mode

Website Group

Description

Assign website object to group.

Options

<WEB_SITE_OBJ_NAME> Website object name.
Example: *Website domain object*

Example

```
website-object "allowed website object"
```

Syntax

```
no website-object <WEB_SITE_OBJ_NAME>
```

Mode

Website Group

Description

Remove website object from group.

Options

<WEB_SITE_OBJ_NAME> Website object name.
Example: *Website domain object*

Example

```
no website-object "website object name"
```

Syntax

```
website-group <WEB_SITE_GRP_NAME>
```

Mode

Website Group

Description

Assign website group to group.

Options

<WEB_SITE_GRP_NAME> Website group name.
Example: *Website domain group*

Example

```
website-group "website group name"
```

Syntax

```
no website-group <WEB_SITE_GRP_NAME>
```

Mode

Website Group

Description

Remove website group from group.

Options

<WEB_SITE_GRP_NAME> Website group name.
Example: *Website domain group*

Example

```
no website-group "website group name"
```

Syntax

```
no website-group-members
```

Mode

Website Group

Description

Remove all members from website-group.

Example

```
no website-group-members
```

Syntax

```
uuid <UUID>
```

Mode

Website Group

Description

Set website group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

```
uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c
```

Syntax

```
no uuid
```

Mode

Website Group

Description

Clear website group UUID.

Example

no uuid

Syntax

no decryption-policy { client | server | ssh } uuid <DEC_POLICY_UUID>

Mode

Config

Description

Delete decryption policy.

Options

<i>client</i>	server.
<i>server</i>	server.
<i>ssh</i>	ssh.
<i>uuid</i>	Delete an decryption policy by UUID.
<i><DEC_POLICY_UUID></i>	Universally Unique Identifier (UUID). Example: <i>550e8400-e29b-41d4-a716-446655440000</i>

Example

no decryption-policy "Office Decryption Policy"

Syntax

no decryption-policies [client | server | ssh]

Mode

Config

Description

Delete all decryption policies.

Options

<i>client</i>	client.
<i>server</i>	server.
<i>ssh</i>	ssh.

Example

no decryption-policies

Syntax

```
decryption-policy { client | server | ssh } uuid <DEC_POLICY_UUID>
```

Mode

Config

Description

Add/Edit decryption policy and enter configuration mode.

Options

client	client.
server	server.
ssh	ssh.
uuid	Edit decryption policy by UUID.
<DEC_POLICY_UUID>	Universally Unique Identifier (UUID). Example: 550e8400-e29b-41d4-a716-446655440000

Example

```
decryption-policy "Office Decryption Policy"
```

Syntax

```
clone decryption-policy { client | server | ssh } uuid <DEC_POLICY_UUID> location { after | before }
```

Mode

Config

Description

Clone decryption policy.

Options

client	client.
server	server.
ssh	ssh.
uuid	clone decryption policy by UUID.
<DEC_POLICY_UUID>	Universally Unique Identifier (UUID). Example: 550e8400-e29b-41d4-a716-446655440000
location	Location to clone decryption policy.
after	Clone decryption policy after.
before	Clone decryption policy before.

Example

```
clone decryption-policy "Office Decryption Policy" location before
```

Syntax

```
uuid <DEC_POLICY_UUID>
```

Mode

Decryption Policy

Description

Decryption policy UUID.

Options

<DEC_POLICY_UUID> Universally Unique Identifier (UUID).
Example: *550e8400-e29b-41d4-a716-446655440000*

Example

uuid 138a224d-c4c7-d621-0a00-c0eae49ce84c

Syntax

no uuid

Mode

Decryption Policy

Description

Clear decryption policy UUID.

Example

no uuid

Syntax

name <WORD>

Mode

Decryption Policy

Description

Decryption policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name OfficeDecryptionPolicy

Syntax

no name

Mode

Decryption Policy

Description

Clear decryption policy name.

Example

no name

Syntax

```
priority { begin | end | manual <UINT32> }
```

Mode

Decryption Policy

Description

Set decryption policy priority.

Options

- begin** Insert the policy at the beginning.
- end** Insert the policy at the end.
- manual** Set manual priority for decryption policy.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHH. Example: 123

Example

```
priority begin
priority manual 1
```

Syntax

```
comment <WORD>
```

Mode

Decryption Policy

Description

Decryption policy comment.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\". Example: abc

Example

```
comment "This decryption policy is only for corp server access"
```

Syntax

```
no comment
```

Mode

Decryption Policy

Description

Clear decryption policy comment.

Example

```
no comment
```

Syntax

```
enable
```

Mode

Description

Enable decryption policy.

Example

enable

Syntax

no enable

Mode

Decryption Policy

Description

Disable decryption policy.

Example

no enable

Syntax

source address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }

Mode

Decryption Policy

Description

Specify a destination for this decryption policy.

Options

<i>any</i>	Any address.
<i>fqdn</i> <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
<i>group</i> <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
<i>host</i> <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>mac</i> <ADDR_MAC>	Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
<i>name</i> <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
<i>network</i> <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>

range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
source address name "Corporate servers"
```

Syntax

```
destination address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Decryption Policy

Description

Specify a destination for this decryption policy.

Options

any	Any address.
fqdn <ADDR_FQDN>	Address object full qualified domain name. FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group <ADDR_GROUP_NAME_MIXED>	Address group name. Group address object name. Example: <i>Sales Group</i>
host <ADDR_HOST>	Address object host. IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac <ADDR_MAC>	Address object mac. Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name <ADDR_NAME_MIXED>	Address object name. Address object name. Example: <i>Web Server</i>
network <ADDR_NETWORK>	Address object network. IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range <ADDR_BEGIN>	Address object range. IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

```
destination address name "Corporate Servers"
```


Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Decryption Policy

Description

Specify a service for this decryption policy.

Options

any	Any destination service.
group	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
name	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
protocol	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
service FTP
```

Syntax

```
users included { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> } }
```

Mode

Decryption Policy

Description

Specify users that apply to this decryption policy.

Options

administrator	Administrator.
all	All users.
group	Group object name.
<LOCAL_USER_GROUP_NAME>	Local user group object name. Example: <i>Limited Administrators</i>
guests	Guest users.
name	User object name.
<LOCAL_USER_NAME>	Local user object name. Example: <i>user1</i>

Example

```
users name "Corporate IT Administrators"
```

Syntax

match-operation { and | or }

Mode

Decryption Policy

Description

Specify the match operation for this decryption policy.

Options

and AND.

or OR.

Example

match-operation and

Syntax

web-category { any | group <WEB_CATEGORY_GRP_NAME> }

Mode

Decryption Policy

Description

Assign web category group to decryption policy.

Options

any Assign any to decryption policy.

group Web category group.

<WEB_CATEGORY_GRP_NAME> Web category group name.
Example: *Web category group*

Example

web-category group "Denied Web Site Group"

Syntax

web-site { any | group <WEB_SITE_GRP_NAME> | name <WEB_SITE_OBJ_NAME> }

Mode

Decryption Policy

Description

Assign Web site to decryption policy.

Options

any Assign any to decryption policy.

group Web site group.

<WEB_SITE_GRP_NAME> Website group name.
Example: *Website domain group*

name Web site object name.

<WEB_SITE_OBJ_NAME> Website object name.
Example: *Website domain object*

Example

web-site group "Denied URL Group"

Syntax

country { any | group <COUNTRY_GROUP_NAME> }

Mode

Decryption Policy

Description

Assign country group to decryption policy.

Options

- any** Assign any to decryption policy.
- group** Country group.
- <COUNTRY_GROUP_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

country group "Denied Country Group"

Syntax

schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } }

Mode

Decryption Policy

Description

Specify a schedule for this decryption policy.

Options

- always-on** Always on.
- days** Schedule object days.
- <SCHED_DAYS>** Days of the week in the form: SU-M-T-W-TH-F-SA.
Example: *SU-M-TH-SA*
- time** Schedule object beginning/ending time.
- <SCHED_TIME_BEGIN>** Time in the form: DD:DD.
Example: *12:00*
- <SCHED_TIME_END>** Time in the form: DD:DD.
Example: *12:00*
- name** Schedule object name.
- <SCHED_NAME>** Schedule object name.
Example: *Work Hours*

Example

schedule name "IT Maintenance"

Syntax

```
action { { bypass | decrypt } }
```

Mode

Decryption Policy

Description

Set the action for this decryption policy.

Options

bypass Bypass traffic matching the criteria.

decrypt Decrypt traffic matching the criteria.

Example

```
action decrypt
```

Syntax

```
ticket { tag1 <WORD> | tag2 <WORD> | tag3 <WORD> }
```

Mode

Decryption Policy

Description

Set decryption policy ticket tag.

Options

tag1 Set decryption policy profile ticket tag1.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

tag2 Set decryption policy profile ticket tag2.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

tag3 Set decryption policy profile ticket tag3.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ticket tag1 "Tag number 1"
```

Syntax

```
no ticket { tag1 | tag2 | tag3 }
```

Mode

Decryption Policy

Description

Clear decryption policy ticket tag.

Options

tag1 Set decryption policy profile ticket tag1.

tag2 Set decryption policy profile ticket tag2.

tag3 Set decryption policy profile ticket tag3.

Example

```
no ticket tag1
```

Syntax

```
ip-type { ipv4 | ipv6 }
```

Mode

Decryption Policy

Description

Ip version.

Options

ipv4 ipv4.

ipv6 ipv6.

Example

```
ip-type ipv4
```

Syntax

```
clear decryption-policy uuid <DEC_POLICY_UUID> statistics
```

Mode

Config

Description

Clear firewall decryption policy statistics by UUID.

Options

uuid	uuid
<DEC_POLICY_UUID>	Universally Unique Identifier (UUID). Example: 550e8400-e29b-41d4-a716-446655440000
statistics	Clear firewall decryption policy statistics by UUID.

Example

```
clear decryption-policy uuid 00000000-0000-0001-1e00-2cb8ed4acd38 statistics
```

Syntax

```
clear decryption-policies statistics
```

Mode

Config

Description

Clear firewall decryption policies statistics.

Options

statistics Clear firewall decryption policies statistics.

Example

```
clear decryption-policies statistics
```

Syntax

```
no country-group [ uuid ] <COUNTRY_GROUP_NAME>
```

Mode

Config

Description

Delete a country group.

Options

uuid	Delete a country group by UUID.
<COUNTRY_GROUP_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>China</i>

Example

```
no country-group "Allowed Countries"
```

Syntax

```
no country-groups
```

Mode

Config

Description

Delete all custom country groups.

Example

```
no country-groups
```

Syntax

```
country-group [ uuid ] <COUNTRY_GROUP_NAME>
```

Mode

Config

Description

Add/edit country group and enter configuration mode.

Options

uuid	Edit a country group by UUID.
<COUNTRY_GROUP_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>China</i>

Example

```
country-group "Allowed Countries"
```

Syntax

name <COUNTRY_GROUP_NAME>

Mode

Country Group

Description

Set country group name.

Options

<COUNTRY_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

name "Allowed Countries "

Syntax

uuid <UUID>

Mode

Country Group

Description

Set country group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Country Group

Description

Clear country group UUID.

Example

no uuid

Syntax

no country <COUNTRY_OBJECT_NAME>

Mode

Country Group

Description

Remove country from group.

Options

<COUNTRY_OBJECT_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

```
no country "New Zealand"
```

Syntax

```
no countries
```

Mode

Country Group

Description

Remove all contries from group.

Example

```
no countries
```

Syntax

```
country <COUNTRY_OBJECT_NAME>
```

Mode

Country Group

Description

Assign country to group.

Options

<COUNTRY_OBJECT_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

```
country "New Zealand"
```

Syntax

```
no country-group <COUNTRY_GROUP_NAME>
```

Mode

Country Group

Description

Remove country group from group.

Options

<COUNTRY_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

```
no country-group "North American Countries"
```

Syntax

no country-groups

Mode

Country Group

Description

Remove all country group from group.

Example

no country-groups

Syntax

country-group <COUNTRY_GROUP_NAME>

Mode

Country Group

Description

Assign country group to group.

Options

<COUNTRY_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *China*

Example

country-group "North American Contries"

Syntax

security-policies max-count <UINT32>

Mode

Config

Description

Set max security policies count.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

access-rules max-count 800

Syntax

no security-policies { ipv4 | ipv6 }

Mode

Config

Description

Delete all security policies.

Options

- ipv4** IPv4 security policy.
- ipv6** IPv6 security policy.

Example

```
no security-policies ipv4
```

Syntax

```
no security-policy ipv4 uuid <SECURITY_POLICY_UUID>
```

Mode

Config

Description

Delete security policy.

Options

- uuid** Delete a security policy by UUID.
- <SECURITY_POLICY_UUID>** Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38

Example

```
no security-policy ipv4 uuid 00000000-0000-0001-0700-2cb8ed4acd38
```

Syntax

```
security-policy ipv4 uuid <SECURITY_POLICY_UUID>
```

Mode

Config

Description

Add/Edit security policy and enter configuration mode.

Options

- uuid** Edit security policy by UUID.
- <SECURITY_POLICY_UUID>** Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38

Example

```
security-policy ipv4 uuid 00000000-0000-0001-0700-2cb8ed4acd38
```

Syntax

```
no security-policy ipv6 uuid <SECURITY_POLICY_UUID>
```

Mode

Config

Description

Delete an IPv6 security policy.

Options

uuid Delete a security policy by UUID.
<SECURITY_POLICY_UUID> Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38

Example

no security-policy ipv6 uuid 00000000-0000-0002-0700-2cb8ed4acd38

Syntax

security-policy ipv6 uuid <SECURITY_POLICY_UUID>

Mode

Config

Description

Add/Edit security policy and enter configuration mode.

Options

uuid Edit security policy by UUID.
<SECURITY_POLICY_UUID> Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38

Example

security-policy ipv6 uuid 00000000-0000-0002-0700-2cb8ed4acd38

Syntax

clone security-policy ipv4 uuid <SECURITY_POLICY_UUID> location { after | before }

Mode

Config

Description

Clone security policy.

Options

uuid Clone security policy by UUID.
<SECURITY_POLICY_UUID> Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38
location Location to clone security policy policy.
after Clone security policy policy after.
before Clone security policy policy before.

Example

clone security-policy ipv4 uuid 00000000-0000-0001-0700-2cb8ed4acd38 location before

Syntax

clone security-policy ipv6 uuid <SECURITY_POLICY_UUID> location { after | before }

Mode

Config

Description

Clone security policy.

Options

uuid	Clone security policy by UUID.
<SECURITY_POLICY_UUID>	Security policy UUID. Example: 00000000-0000-0001-0700-2cb8ed4acd38
location	Location to clone security policy policy.
after	Clone security policy policy after.
before	Clone security policy policy before.

Example

```
clone security-policy ipv6 uuid 00000000-0000-0002-0700-2cb8ed4acd38 location before
```

Syntax

```
clear security-policies statistics
```

Mode

Config

Description

Clear firewall security policies statistics.

Syntax

```
clear security-policy ipv4 uuid <SECURITY_POLICY_UUID> statistics
```

Mode

Config

Description

Clear security policy statistics by UUID.

Options

uuid	Clear security policy statistics by UUID.
<SECURITY_POLICY_UUID>	Security policy UUID. Example: 00000000-0000-0001-0700-2cb8ed4acd38
statistics	Clear security policy statistics by UUID.

Syntax

```
clear security-policy ipv6 uuid <SECURITY_POLICY_UUID> statistics
```

Mode

Config

Description

Clear security policy statistics by UUID.

Options

uuid	Clear security policy statistics by UUID.
<SECURITY_POLICY_UUID>	Security policy UUID. Example: 00000000-0000-0001-0700-2cb8ed4acd38
statistics	Clear security policy statistics by UUID.

Syntax

uuid <SECURITY_POLICY_UUID>

Mode

Security Policy
Security Policy IPv6

Description

Security policy UUID.

Options

<SECURITY_POLICY_UUID> Security policy UUID.
Example: 00000000-0000-0001-0700-2cb8ed4acd38

Example

uuid 00000000-0000-0001-0700-2cb8ed4acd38

Syntax

no uuid

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy UUID.

Example

no uuid

Syntax

name <WORD>

Mode

Security Policy
Security Policy IPv6

Description

Security policy name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name OfficePolicy

Syntax

no name

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy name.

Example

no name

Syntax

priority { begin | end | manual <UINT32> }

Mode

Security Policy
Security Policy IPv6

Description

Set security policy priority.

Options

- begin*** Insert the policy at the beginning.
- end*** Insert the policy at the end.
- manual*** Set manual priority for security policy.
- <UINT32>*** Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

priority begin
priority manual 1

Syntax

no priority manual

Mode

Security Policy
Security Policy IPv6

Description

Clear access rule priority.

Options

- manual*** Set manual priority for access rule.

Example

no priority manual

Syntax

comment <WORD>

Mode

Security Policy
Security Policy IPv6

Description

Security policy comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "This security policy is only for corp client access"
```

Syntax

```
no comment
```

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy comment.

Example

```
no comment
```

Syntax

```
enable
```

Mode

Security Policy
Security Policy IPv6

Description

Enable security policy.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Security Policy
Security Policy IPv6

Description

Disable security policy.

Example

```
no enable
```

Syntax

```
from <SECURITY_POLICY_ZONE_NAME>
```

Mode

Description

Specify a source zone for this security policy.

Options

<SECURITY_POLICY_ZONE_NAME> Security policy zone name.
Example: *DMZ*

Example

from LAN

Syntax

to <SECURITY_POLICY_ZONE_NAME>

Mode

Security Policy
Security Policy IPv6

Description

Specify a destination zone for this security policy.

Options

<SECURITY_POLICY_ZONE_NAME> Security policy zone name.
Example: *DMZ*

Example

to X2

Syntax

source address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }

Mode

Security Policy
Security Policy IPv6

Description

Specify a source for this security policy.

Options

any Any address.

fqdn Address object full qualified domain name.
<ADDR_FQDN> FQDN in the form: example.com or *.example.com.
Example: *example.com*

group Address group name.
<ADDR_GROUP_NAME_WITH_MIXED> Group address object name.
Example: *Sales Group*

host Address object host.
<ADDR_HOST> IPV4: address object IPv4 host address in the form: D.D.D.D\nIPV6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n.
Example: *IPV4: 192.168.168.168\nIPV6: 2001:cdba:0000:0000:0000:0000:3257:9652\n*

mac Address object mac.

<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>
range	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:effe\n</i>

Example

source address name "Corporate Servers"

Syntax

```
destination address { { any | fqdn <ADDR_FQDN> | group <ADDR_GROUP_NAME_WITH_MIXED> | host <ADDR_HOST> | mac <ADDR_MAC> | name <ADDR_NAME_WITH_MIXED> | network <ADDR_NETWORK> <ADDR_MASK> | range <ADDR_BEGIN> <ADDR_END> } }
```

Mode

Security Policy
Security Policy IPv6

Description

Specify a destination for this security policy.

Options

any	Any address.
fqdn	Address object full qualified domain name.
<ADDR_FQDN>	FQDN in the form: example.com or *.example.com. Example: <i>example.com</i>
group	Address group name.
<ADDR_GROUP_NAME_WITH_MIXED>	Group address object name. Example: <i>Sales Group</i>
host	Address object host.
<ADDR_HOST>	IPv4: address object IPv4 host address in the form: D.D.D.D\nIPv6: address object IPv6 host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.168\nIPv6: 2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
mac	Address object mac.
<ADDR_MAC>	Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.
name	Address object name.
<ADDR_NAME_WITH_MIXED>	Address object name. Example: <i>Web Server</i>
network	Address object network.
<ADDR_NETWORK>	IPv4: address object IPv4 network in the form: D.D.D.D\nIPv6: address object IPv6 network in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.168.0\nIPv6: 2001:cdba:3257:effe:0000:0000:0000:0000\n</i>
<ADDR_MASK>	IPv4: address object IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D\nIPv6: address object IPv6 netmask in the form: /D\n. Example: <i>IPv4: 255.255.255.0\nIPv6: /64\n</i>

<i>range</i>	Address object range.
<ADDR_BEGIN>	IPv4: address object IPv4 starting range in the form: D.D.D.D\nIPv6: address object IPv6 starting range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.100\nIPv6: 2001:cdba:0000:0000:0000:3257:9652\n</i>
<ADDR_END>	IPv4: address object IPv4 ending range in the form: D.D.D.D\nIPv6: address object IPv6 ending range in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>IPv4: 192.168.1.150\nIPv6: 2001:cdba:0000:0000:0000:3257:effe\n</i>

Example

destination address name "Corporate Servers"

Syntax

```
service { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Security Policy
Security Policy IPv6

Description

Specify a service for this security policy.

Options

<i>any</i>	Any destination service.
<i>group</i>	Service group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>
<i>name</i>	Service object name.
<SVC_NAME>	Service object name. Example: <i>HTTPS</i>
<i>protocol</i>	Service object protocol.
<SVC_PROTOCOL>	Service protocol. Example: <i>TCP</i>
<SVC_PORT_BEGIN>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<SVC_PORT_END>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

service FTP

Syntax

```
source port { { any | group <SVC_GROUP_NAME> | name <SVC_NAME> | protocol <SVC_PROTOCOL> <SVC_PORT_BEGIN> <SVC_PORT_END> } }
```

Mode

Security Policy
Security Policy IPv6

Description

Specify a source port for this security policy.

Options

<i>any</i>	Any source service.
<i>group</i>	Source service Group name.
<SVC_GROUP_NAME>	Service object group name. Example: <i>VOIP</i>

<i>name</i>	Source service Object name.
<i><SVC_NAME></i>	Service object name. Example: <i>HTTPS</i>
<i>protocol</i>	Source service Object protocol.
<i><SVC_PROTOCOL></i>	Service protocol. Example: <i>TCP</i>
<i><SVC_PORT_BEGIN></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i><SVC_PORT_END></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

```
source port name "Corporate IT Administration"
```

Syntax

```
users { { administrator | all | group <LOCAL_USER_GROUP_NAME> | guests | name <LOCAL_USER_NAME> } }
```

Mode

Security Policy
Security Policy IPv6

Description

Specify users that apply to this security policy.

Options

<i>administrator</i>	Administrator.
<i>all</i>	All users.
<i>group</i>	Group object name.
<i><LOCAL_USER_GROUP_NAME></i>	Local user group object name. Example: <i>Limited Administrators</i>
<i>guests</i>	Guest users.
<i>name</i>	User object name.
<i><LOCAL_USER_NAME></i>	Local user object name. Example: <i>user1</i>

Example

```
users name "Corporate IT Administrators"
```

Syntax

```
match-operation { and | or }
```

Mode

Security Policy
Security Policy IPv6

Description

Specify the match operation for this security policy.

Options

<i>and</i>	AND.

or OR.

Example

match-operation and

Syntax

application { any | group <APP_GROUP_NAME> }

Mode

Security Policy
Security Policy IPv6

Description

Assign application group to security policy.

Options

- any** Assign any to security policy.
- group** Application group.
- <APP_GROUP_NAME>** Atom Object name.
Example: *Application Tech Apps*

Example

application group "Severe Risk App Group"

Syntax

and-all-matched-applications

Mode

Security Policy
Security Policy IPv6

Description

Enable AND all matched applications.

Example

and-all-matched-applications

Syntax

no and-all-matched-applications

Mode

Security Policy
Security Policy IPv6

Description

Disable AND all matched applications.

Example

no and-all-matched-applications

Syntax

```
web-category { any | group <WEB_CATEGORY_GRP_NAME> }
```

Mode

Security Policy
Security Policy IPv6

Description

Assign web category group to security policy.

Options

- any** Assign any to security policy.
- group** Web category group.
- <WEB_CATEGORY_GRP_NAME>** Web category group name.
Example: *Web category group*

Example

```
web-category group "Denied Web Site Group"
```

Syntax

```
url-list { any | group <CONTENT_FILTER_URI_LIST_GRP_NAME> | name <CONTENT_FILTER_URI_LIST_OBJ_NAME> }
```

Mode

Security Policy
Security Policy IPv6

Description

Assign URL list to security policy.

Options

- any** Assign any to security policy.
- group** URL list group.
- <CONTENT_FILTER_URI_LIST_GRP_NAME>** Content filter URI list group name.
Example: *White URI list group*
- name** URL list object name.
- <CONTENT_FILTER_URI_LIST_OBJ_NAME>** Content filter URI list object name.
Example: *White URI list object*

Example

```
url-list group "Denied URL Group"
```

Syntax

```
custom-match { any | group <CUSTOM_MATCH_GROUP_NAME> }
```

Mode

Security Policy
Security Policy IPv6

Description

Assign custom match to security policy.

Options

any	Assign any to security policy.
group	Custom match group.
<CUSTOM_MATCH_GROUP_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

custom-match group "Denied File Content Group"

Syntax

country { any | group <COUNTRY_GROUP_NAME> }

Mode

Security Policy
Security Policy IPv6

Description

Assign country group to security policy.

Options

any	Assign any to security policy.
group	Country group.
<COUNTRY_GROUP_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>China</i>

Example

country group "Denied Country Group"

Syntax

schedule { { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> } }

Mode

Security Policy
Security Policy IPv6

Description

Specify a schedule for this security policy.

Options

always-on	Always on.
days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending days.time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule name "IT Maintenance"
```

Syntax

```
action { { allow | deny | discard } }
```

Mode

Security Policy
Security Policy IPv6

Description

Set the action for this security policy.

Options

allow Allow traffic matching the criteria.

deny Deny traffic matching the criteria.

discard Discard traffic matching the criteria.

Example

```
action allow
```

Syntax

```
action-profile <SECURITY_ACTION_PROFILE_NAME>
```

Mode

Security Policy
Security Policy IPv6

Description

Assign action profile to security policy.

Options

<SECURITY_ACTION_PROFILE_NAME> Security action profile name.
Example: *MySecurityActionProfile*

Example

```
action-profile "Corp Threat Action Profile"
```

Syntax

```
no action-profile
```

Mode

Security Policy
Security Policy IPv6

Description

Clear action profile to security policy.

Example

```
no action-profile
```

Syntax

ticket tag1 <WORD>

Mode

Security Policy
Security Policy IPv6

Description

Set security policy ticket tag 1.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ticket tag1 "Tag number 1"

Syntax

no ticket tag1

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy ticket tag.

Example

no ticket tag1

Syntax

ticket tag2 <WORD>

Mode

Security Policy
Security Policy IPv6

Description

Set security policy ticket tag 2.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ticket tag2 "Tag number 2"

Syntax

no ticket tag2

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy ticket tag 2.

Example

no ticket tag1

Syntax

ticket tag3 <WORD>

Mode

Security Policy
Security Policy IPv6

Description

Set security policy ticket tag 3.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ticket tag3 "Tag number 3"

Syntax

no ticket tag3

Mode

Security Policy
Security Policy IPv6

Description

Clear security policy ticket tag 3.

Example

no ticket tag3

Syntax

policy section uuid <POLICY_SECTION_UUID> name <POLICY_SECTION_NAME>

Mode

Config

Description

Add policy section.

Options

uuid	Policy by UUID.
<POLICY_SECTION_UUID>	Policy section UUID. Example: <i>00000000-0000-0001-0700-2cb8ed4acd38</i>
name	Section name.
<POLICY_SECTION_NAME>	Policy section name. Example: <i>test</i>

Example

```
policy section uuid 00000000-0000-0001-0700-2cb8ed4acd38 name mySection
```

Syntax

```
no policy section uuid <POLICY_SECTION_UUID> name <POLICY_SECTION_NAME>
```

Mode

Config

Description

Delete a policy section by policy uuid.

Options

uuid	Policy by UUID.
<POLICY_SECTION_UUID>	Policy section UUID. Example: <i>00000000-0000-0001-0700-2cb8ed4acd38</i>
name	Section name.
<POLICY_SECTION_NAME>	Policy section name. Example: <i>test</i>

Example

```
no policy section uuid 00000000-0000-0001-0700-2cb8ed4acd38 name test
```

Syntax

```
no policy sections
```

Mode

Config

Description

Delete all policy sections.

Example

```
no policy section uuid 00000000-0000-0001-0700-2cb8ed4acd38
```

Syntax

```
uuid <POLICY_SECTION_UUID>
```

Mode

Policy Section

Description

Set policy section policy UUID.

Options

<POLICY_SECTION_UUID>	Policy section UUID. Example: <i>00000000-0000-0001-0700-2cb8ed4acd38</i>

Example

```
uuid 00000000-0000-0001-0700-2cb8ed4acd38
```

Syntax

name <POLICY_SECTION_NAME>

Mode

Policy Section

Description

Set policy section name.

Options

<POLICY_SECTION_NAME> Policy section name.
Example: test

Example

name mySection

Syntax

no web-category-groups

Mode

Config

Description

Delete all web category groups.

Example

no web-category-groups

Syntax

no web-category-group [uuid] <WEB_CATEGORY_GRP_NAME>

Mode

Config

Description

Delete a web category group.

Options

uuid Select web category group by UUID.
<WEB_CATEGORY_GRP_NAME> Web category group name.
Example: Web category group

Example

no web-category-group "webCategoryGrpName"

Syntax

web-category-group [uuid] <WEB_CATEGORY_GRP_NAME>

Mode

Config

Description

Add/Edit web category group and enter configuration mode.

Options

- `uuid` Select web category group by UUID.
- `<WEB_CATEGORY_GRP_NAME>` Web category group name.
Example: *Web category group*

Example

web-category-group "Web Category Group Name"

Syntax

name <WEB_CATEGORY_GRP_NAME>

Mode

Web Category Group

Description

Set web category group name.

Options

- `<WEB_CATEGORY_GRP_NAME>` Web category group name.
Example: *Web category group*

Example

name "default group name"

Syntax

web-category-object <WEB_CATEGORY_OBJ_NAME>

Mode

Web Category Group

Description

Assign web category object to group.

Options

- `<WEB_CATEGORY_OBJ_NAME>` Web category object name.
Example: *Web category object*

Example

web-category-object "allowed web category object"

Syntax

no web-category-object <WEB_CATEGORY_OBJ_NAME>

Mode

Web Category Group

Description

Remove web category object from group.

Options

- `<WEB_CATEGORY_OBJ_NAME>` Web category object name.
Example: *Web category object*

Example

```
no web-category-object "web category object name"
```

Syntax

```
web-category-group <WEB_CATEGORY_GRP_NAME>
```

Mode

Web Category Group

Description

Assign web category group to group.

Options

<WEB_CATEGORY_GRP_NAME> Web category group name.
Example: *Web category group*

Example

```
web-category-group "web category group name"
```

Syntax

```
no web-category-group <WEB_CATEGORY_GRP_NAME>
```

Mode

Web Category Group

Description

Remove web category group from group.

Options

<WEB_CATEGORY_GRP_NAME> Web category group name.
Example: *Web category group*

Example

```
no web-category-group "web category group name"
```

Syntax

```
no web-category-group-members
```

Mode

Web Category Group

Description

Remove all members from web-category-group.

Example

```
no web-category-group-members
```

Syntax

```
uuid <UUID>
```

Mode

Web Category Group

Description

Set web category group UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Web Category Group

Description

Clear web category group UUID.

Example

no uuid

Syntax

no threat-prevention-profile [uuid] <THREAT_PROFILE_NAME>

Mode

Config

Description

Delete a threat prevention profile.

Options

uuid Delete a threat prevention profile by UUID.
<THREAT_PROFILE_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *DNS Category Profile*

Example

no threat-prevention-profile "Threat Prevention Signature Profile"

Syntax

no threat-prevention-profiles

Mode

Config

Description

Delete all custom threat prevention profiles.

Example

no threat-prevention-profiles

Syntax

threat-prevention-profile [uuid] <THREAT_PROFILE_NAME>

Mode

Config

Description

Add/edit threat prevention profile and enter configuration mode.

Options

- uuid** Edit a threat prevention profile by UUID.
- <THREAT_PROFILE_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *DNS Category Profile*

Example

threat-prevention-profile "Threat Prevention Signature Profile"

Syntax

name <THREAT_PROFILE_NAME>

Mode

Threat Prevention Profile

Description

Set threat prevention profile name.

Options

- <THREAT_PROFILE_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *DNS Category Profile*

Example

name "Threat Prevention Signature Profile"

Syntax

uuid <UUID>

Mode

Threat Prevention Profile

Description

Set threat prevention profile UUID.

Options

- <UUID>** Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Threat Prevention Profile

Description

Clear threat prevention profile UUID.

Example

no uuid

Syntax

negate

Mode

Threat Prevention Profile

Description

Enable threat prevention profile negate.

Example

negate

Syntax

no negate

Mode

Threat Prevention Profile

Description

Disable threat prevention profile negate.

Example

no negate

Syntax

no threat-prevention-object <WORD>

Mode

Threat Prevention Profile

Description

Remove threat prevention object from profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no threat-prevention-object "ABB Test Signal Viewer ActiveX Arbitrary File Overwrite 2"

Syntax

```
no threat-prevention-objects
```

Mode

Threat Prevention Profile

Description

Remove all threat prevention objects from profile.

Example

```
no threat-prevention-objects
```

Syntax

```
threat-prevention-object <WORD>
```

Mode

Threat Prevention Profile

Description

Assign threat prevention object to profile.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
threat-prevention-object "ABB Test Signal Viewer ActiveX Arbitrary File Overwrite 2"
```

Syntax

```
policies-setting
```

Mode

Config

Description

Enter policies setting configuration mode.

Example

```
policies-setting
```

Syntax

```
enforcement { global | policy }
```

Mode

Policies Setting

Description

Set security services enforcements mode.

Options

global Global.

policy Policy.

Example

enforcement policy

Syntax

block-connections application-signatures-unavailable

Mode

Policies Setting

Description

Enable block connections when application signatures are unavailable and rules need application.

Example

block-connections application-signatures-unavailable

Syntax

no block-connections application-signatures-unavailable

Mode

Policies Setting

Description

Disable block connections when application signatures are unavailable and rules need application.

Example

no block-connections application-signatures-unavailable

Syntax

block-connections malware-databases-not-downloaded

Mode

Policies Setting

Description

Enable block connections when Anti-Malware databases are not downloaded and rules need Malware info.

Example

block-connections malware-databases-not-downloaded

Syntax

no block-connections malware-databases-not-downloaded

Mode

Policies Setting

Description

Disable block connections when Anti-Malware databases are not downloaded and rules need Malware info.

Example

```
no block-connections malware-databases-not-downloaded
```

Syntax

```
active-application-caching
```

Mode

Policies Setting

Description

Enable active application caching.

Example

```
active-application-caching
```

Syntax

```
no active-application-caching
```

Mode

Policies Setting

Description

Disable active application caching.

Example

```
no active-application-caching
```

Syntax

```
cached-application-bypass
```

Mode

Policies Setting

Description

Enable cached applications to bypass DPI.

Example

```
cached-application-bypass
```

Syntax

```
no cached-application-bypass
```

Mode

Policies Setting

Description

Disable cached applications to bypass DPI.

Example

```
no cached-application-bypass
```

Syntax

```
application-cache default { threshold <UINT16> | timeout <UINT16> }
```

Mode

Policies Setting

Description

Set default application cache.

Options

threshold Set default application cache threshold in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

timeout Set default application cache timeout in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
application-cache default timeout 10
application-cache default threshold 100
```

Syntax

```
no application-cache default timeout
```

Mode

Policies Setting

Description

Clear default application cache timeout.

Example

```
no application-cache-timeout default
```

Syntax

```
application-cache global timeout { enable | value <UINT16> }
```

Mode

Policies Setting

Description

Set global application cache timeout.

Options

enable Enable global application cache timeout.

value Set global application cache timeout in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
application-cache global timeout value 10
application-cache global timeout enable
```

Syntax

```
no application-cache global timeout { enable | value }
```

Mode

Policies Setting

Description

Set global application cache timeout.

Options

enable Disable global application cache timeout.

value Clear global application cache timeout.

Example

```
no application-cache global timeout value
no application-cache global timeout enable
```

Syntax

```
application-cache global threshold { enable | value <UINT16> }
```

Mode

Policies Setting

Description

Set global application cache threshold.

Options

enable Enable global application cache threshold.

value Set global application cache threshold in seconds.

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
application-cache global threshold value 10
application-cache global threshold enable
```

Syntax

```
no application-cache global threshold enable
```

Mode

Policies Setting

Description

Disable global application cache threshold.

Options

enable Disable global application cache threshold.

Example

```
no application-cache global threshold enable
```

Syntax

```
clear app-cache
```

Mode

Policies Setting

Description

Clear app cache.

Example

```
clear app-cache
```

Syntax

```
block-connections geoip-database-not-downloaded
```

Mode

Policies Setting

Description

Enable block connections when Geo IP database is not downloaded and rules need Geo location.

Example

```
block-connections geoip-database-not-downloaded
```

Syntax

```
no block-connections geoip-database-not-downloaded
```

Mode

Policies Setting

Description

Disable block connections when Geo IP database is not downloaded and rules need Geo location.

Example

```
no block-connections geoip-database-not-downloaded
```

Syntax

```
block-connections botnet-signature-not-unavailable
```

Mode

Policies Setting

Description

Enable block connections when BOTNET signatures are unavailable and rules need botnet control.

Example

```
block-connections botnet-signature-not-unavailable
```

Syntax

no block-connections botnet-signature-not-unavailable

Mode

Policies Setting

Description

Disable block connections when BOTNET signatures are unavailable and rules need botnet control.

Example

no block-connections botnet-signature-not-unavailable

Syntax

ssl-server-inspection

Mode

Policies Setting

Description

Enable SSL server inspection.

Example

ssl-server-inspection

Syntax

no ssl-server-inspection

Mode

Policies Setting

Description

Disable SSL server inspection.

Example

no ssl-server-inspection

Syntax

bypass-decryption cfs-not-licensed

Mode

Policies Setting

Description

Enable bypass decryption when CFS is not licensed and rules need web content.

Example

bypass-decryption cfs-not-licensed

Syntax

```
no bypass-decryption cfs-not-licensed
```

Mode

Policies Setting

Description

Disable bypass decryption when CFS is not licensed and rules need web content.

Example

```
no bypass-decryption cfs-not-licensed
```

Syntax

```
bypass-decryption cfs-fail-connect
```

Mode

Policies Setting

Description

Enable bypass decryption when CFS fails to connect to backend rating server and rules need web rating.

Example

```
bypass-decryption cfs-fail-connect
```

Syntax

```
no bypass-decryption cfs-fail-connect
```

Mode

Policies Setting

Description

Disable bypass decryption when CFS fails to connect to backend rating server and rules need web rating.

Example

```
no bypass-decryption cfs-fail-connect
```

Syntax

```
bypass-decryption geoip-database-not-downloaded
```

Mode

Policies Setting

Description

Enable bypass decryption when CFS fails to connect to backend rating server and rules need web rating.

Example

```
bypass-decryption geoip-database-not-downloaded
```

Syntax

```
no bypass-decryption geoip-database-not-downloaded
```


Mode

Policies Setting

Description

Disable bypass decryption when CFS fails to connect to backend rating server and rules need web rating.

Example

```
no bypass-decryption geoip-database-not-downloaded
```

Syntax

```
policy-based-dos-protection
```

Mode

Policies Setting

Description

Enable policy-based DoS protection.

Example

```
policy-based-dos-protection
```

Syntax

```
no policy-based-dos-protection
```

Mode

Policies Setting

Description

Disable policy-based DoS protection.

Example

```
no policy-based-dos-protection
```

Syntax

```
app-custom-malware-mode { global | policy }
```

Mode

Policies Setting

Description

Set application, custom match and malware (threats, virus and spyware) control plus prevention mode.

Options

global Global.

policy Policy.

Example

```
app-custom-malware-mode policy
```

Syntax

```
application-based-on { policy | zone }
```

Mode

Policies Setting

Description

Set what application classification (identification) is based on.

Options

policy Policy.

zone Zone.

Example

```
application-based-on policy
```

Syntax

```
threat-based-on { policy | zone }
```

Mode

Policies Setting

Description

Set what threat detection and prevention is based on.

Options

policy Policy.

zone Zone.

Example

```
threat-based-on policy
```

Syntax

```
antispyware-based-on { policy | zone }
```

Mode

Policies Setting

Description

Set what Anti-Spyware prevention profile is based on.

Options

policy Policy.

zone Zone.

Example

```
antispyware-based-on policy
```

Syntax

```
antivirus-based-on { policy | zone }
```

Mode

Policies Setting

Description

Set what Anti-Virus prevention profile is based on.

Options

policy Policy.

zone Zone.

Example

```
antivirus-based-on policy
```

Syntax

```
geoip-mode { global | policy }
```

Mode

Policies Setting

Description

Set Geo-IP control and enforcement mode.

Options

global Global.

policy Policy.

Example

```
geoip-mode policy
```

Syntax

```
geoip-inspection-based-on { global | policy }
```

Mode

Policies Setting

Description

Set what Geo-IP resolution and inspection is based on.

Options

global Global.

policy Policy.

Example

```
geoip-inspection-based-on policy
```

Syntax

```
botnet-mode { global | policy }
```

Mode

Policies Setting

Description

Set Botnet filter control and enforcement mode.

Options

global Global.

policy Policy.

Example

```
botnet-mode policy
```

Syntax

```
dpissl-mode { global | policy }
```

Mode

Policies Setting

Description

Set decryption (DPI-SSL) control and enforcement mode.

Options

global Global.

policy Policy.

Example

```
dpissl-mode policy
```

Syntax

```
dpissh-mode { global | policy }
```

Mode

Policies Setting

Description

Set decryption (DPI-SSH) control and enforcement mode.

Options

global Global.

policy Policy.

Example

```
dpissh-mode policy
```

Syntax

```
dos-mode { global | policy }
```

Mode

Policies Setting

Description

Set DoS control and enforcement mode.

Options

global Global.

policy Policy.

Example

```
dos-mode policy
```

Syntax

```
syn-flood { global | policy }
```

Mode

Policies Setting

Description

Set SYN flood protection mode.

Options

global Global.

policy Policy.

Example

```
syn-flood policy
```

Syntax

```
udp-flood { global | policy }
```

Mode

Policies Setting

Description

Set UDP flood protection mode.

Options

global Global.

policy Policy.

Example

```
udp-flood policy
```

Syntax

```
icmp-flood { global | policy }
```

Mode

Policies Setting

Description

Set ICMP flood protection mode.

Options

global Global.

policy Policy.

Example

```
icmp-flood policy
```

Syntax

```
attack { global | policy }
```

Mode

Policies Setting

Description

Set attack protection mode.

Options

global Global.

policy Policy.

Example

```
attack policy
```

Syntax

```
ddos { global | policy }
```

Mode

Policies Setting

Description

Set DDoS protection mode.

Options

global Global.

policy Policy.

Example

```
ddos policy
```

Syntax

threat-profile-for-zone

Mode

Policies Setting

Description

Enter global threat profile for zone mode.

Example

threat-profile-for-zone

Syntax

based-on { global | object }

Mode

Global Threat Prevention Profile for zone mode

Description

Set what threat profile is based on.

Options

global Global settings.

object Object settings.

Example

based-on object

Syntax

prevent enable

Mode

Global Threat Prevention Profile for zone mode

Description

Enable prevent.

Example

prevent enable

Syntax

no prevent enable

Mode

Global Threat Prevention Profile for zone mode

Description

Disable prevent.

Example

no prevent enable

Syntax

prevent profile { all | group <THREAT_PROFILE_NAME> }

Mode

Global Threat Prevention Profile for zone mode

Description

Assign threat object group to threat profile prevention.

Options

<i>all</i>	Assign all to threat profile prevention.
<i>group</i>	Threat object group.
<i><THREAT_PROFILE_NAME></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>DNS Category Profile</i>

Example

prevent profile group "Corp Access Threat Group"

Syntax

packet-monitor enable

Mode

Global Threat Prevention Profile for zone mode

Description

Enable threat profile packet monitor.

Example

packet-monitor enable

Syntax

no packet-monitor enable

Mode

Global Threat Prevention Profile for zone mode

Description

Disable threat profile packet monitor.

Example

no packet-monitor enable

Syntax

packet-monitor profile { all | group <THREAT_PROFILE_NAME> }

Mode

Global Threat Prevention Profile for zone mode

Description

Assign threat object group to threat profile packet monitor.

Options

all	Assign all to threat profile packet monitor.
group	Threat object group.
<THREAT_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>DNS Category Profile</i>

Example

packet-monitor profile group "Corp Access Threat Group"

Syntax

log enable

Mode

Global Threat Prevention Profile for zone mode

Description

Enable threat profile log.

Example

log enable

Syntax

no log enable

Mode

Global Threat Prevention Profile for zone mode

Description

Disable threat profile log.

Example

no log enable

Syntax

log profile { all | group <THREAT_PROFILE_NAME> }

Mode

Global Threat Prevention Profile for zone mode

Description

Assign threat object group to threat profile log.

Options

all	Assign all to threat profile log.
group	Threat object group.
<THREAT_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\".

Example

```
log profile group "Corp Access Threat Group"
```

Syntax

```
log redundancy <UINT32>
```

Mode

Global Threat Prevention Profile for zone mode

Description

Set the log redundancy filter interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
log redundancy 3
```

Syntax

```
no log redundancy
```

Mode

Global Threat Prevention Profile for zone mode

Description

Clear the log redundancy filter interval.

Example

```
no log redundancy
```

Syntax

```
high-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Enable signature group high priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i> <UINT32>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: <i>123</i>
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
high-priority prevent-all
high-priority log-redundancy 60
```

Syntax

```
medium-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Enable signature group medium priority detection and log redundancy.

Options

log-all	Log all.
log-redundancy <UINT32>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
packet-monitor-all	Packet monitor all.
prevent-all	Prevent all.

Example

```
medium-priority prevent-all
medium-priority log-redundancy 60
```

Syntax

```
low-priority { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Enable signature group low priority detection and log redundancy.

Options

log-all	Log all.
log-redundancy <UINT32>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
packet-monitor-all	Packet monitor all.
prevent-all	Prevent all.

Example

```
low-priority prevent-all
low-priority log-redundancy 60
```

Syntax

```
no high-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Disable signature group high priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no high-priority prevent-all
no high-priority log-redundancy
```

Syntax

```
no medium-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Disable signature group medium priority detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no medium-priority prevent-all
no medium-priority log-redundancy
```

Syntax

```
no low-priority { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Threat Prevention Profile for zone mode

Description

Disable signature group low priority detection and log redundancy.

Options

<i>log-all</i>	Log all.

log-redundancy Clear log redundancy.

packet-monitor-all Packet monitor all.

prevent-all Prevent all.

Example

```
no low-priority prevent-all
no low-priority log-redundancy
```

Syntax

antispyware-profile-for-zone

Mode

Policies Setting

Description

Enter global Anti-Spyware Prevention profile for zone mode.

Example

antispyware-profile-for-zone

Syntax

inbound

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable inbound inspection.

Example

inbound

Syntax

no inbound

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable inbound inspection.

Example

no inbound

Syntax

outbound

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable outbound inspection.

Example

```
outbound
```

Syntax

```
no outbound
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable outbound inspection.

Example

```
no outbound
```

Syntax

```
smtp-responses
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable SMTP responses.

Example

```
smtp-responses
```

Syntax

```
no smtp-responses
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable SMTP responses.

Example

```
no smtp-responses
```

Syntax

```
http-clientless-notification
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable anti-spyware http clientless notification.

Example

```
http-clientless-notification
```

Syntax

```
no http-clientless-notification
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable anti-spyware http clientless notification.

Example

```
no http-clientless-notification
```

Syntax

```
based-on { global | object }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Set what Anti-Spyware profile is based on.

Options

global Global settings.

object Object settings.

Example

```
based-on object
```

Syntax

```
prevent
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable prevent.

Example

```
prevent
```

Syntax

```
no prevent
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable prevent.

Example

```
no prevent
```

Syntax

```
packet-monitor
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable Anti-Spyware profile packet monitor.

Example

```
packet-monitor
```

Syntax

```
no packet-monitor
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable Anti-Spyware profile packet monitor.

Example

```
no packet-monitor
```

Syntax

```
log enable
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable Anti-Spyware profile log.

Example

```
log enable
```

Syntax

```
no log enable
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable Anti-Spyware profile log.

Example

no log enable

Syntax

log redundancy <UINT32>

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Set the log redundancy filter interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

log redundancy 3

Syntax

no log redundancy

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Clear the log redundancy filter interval.

Example

no log redundancy

Syntax

high-danger { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable signature group high danger detection and log redundancy.

Options

- log-all* Log all.
- log-redundancy <UINT32>* Set log redundancy in seconds.
Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*
- packet-monitor-all* Packet monitor all.
- prevent-all* Prevent all.

Example

```
high-danger prevent-all
high-danger log-redundancy 60
```

Syntax

```
medium-danger { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable signature group medium danger detection and log redundancy.

Options

log-all	Log all.
log-redundancy <UINT32>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
packet-monitor-all	Packet monitor all.
prevent-all	Prevent all.

Example

```
medium-danger prevent-all
medium-danger log-redundancy 60
```

Syntax

```
low-danger { log-all | log-redundancy <UINT32> | packet-monitor-all | prevent-all }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Enable signature group low danger detection and log redundancy.

Options

log-all	Log all.
log-redundancy <UINT32>	Set log redundancy in seconds. Integer in the form: D OR 0xHHHHHHHHH. Example: 123
packet-monitor-all	Packet monitor all.
prevent-all	Prevent all.

Example

```
low-danger prevent-all
low-danger log-redundancy 60
```

Syntax

```
no high-danger { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable signature group high danger detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no high-danger prevent-all
no high-danger log-redundancy
```

Syntax

```
no medium-danger { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable signature group medium danger detection and log redundancy.

Options

<i>log-all</i>	Log all.
<i>log-redundancy</i>	Clear log redundancy.
<i>packet-monitor-all</i>	Packet monitor all.
<i>prevent-all</i>	Prevent all.

Example

```
no medium-danger prevent-all
no medium-danger log-redundancy
```

Syntax

```
no low-danger { log-all | log-redundancy | packet-monitor-all | prevent-all }
```

Mode

Global Anti-Spyware Prevention Profile for zone mode

Description

Disable signature group low danger detection and log redundancy.

Options

<i>log-all</i>	Log all.

log-redundancy Clear log redundancy.

packet-monitor-all Packet monitor all.

prevent-all Prevent all.

Example

```
no low-danger prevent-all
no low-danger log-redundancy
```

Syntax

antivirus-profile-for-zone

Mode

Policies Setting

Description

Enter global Anti-Virus Prevention profile for zone mode.

Example

antivirus-profile-for-zone

Syntax

cloud

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable cloud gateway anti-virus database.

Example

cloud

Syntax

no cloud

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable cloud gateway anti-virus database.

Example

no cloud

Syntax

inbound

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable inbound inspection.

Example

inbound

Syntax

no inbound

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable inbound inspection.

Example

no inbound

Syntax

outbound

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable outbound inspection.

Example

outbound

Syntax

no outbound

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable outbound inspection.

Example

no outbound

Syntax

prevent

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable prevention.

Example

```
prevent
```

Syntax

```
no prevent
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable prevention.

Example

```
no prevent
```

Syntax

```
packet-monitor
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable packet monitor.

Example

```
packet-monitor
```

Syntax

```
no packet-monitor
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable packet monitor.

Example

```
no packet-monitor
```

Syntax

```
log enable
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable log.

Example

log enable

Syntax

no log enable

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable log.

Example

no log enable

Syntax

log redundancy <UINT32>

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Set the log redundancy filter interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

log redundancy 3

Syntax

no log redundancy

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Clear the log redundancy filter interval.

Example

no log redundancy

Syntax

password-protected-zip

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable restricting transfer of password-protected ZIP files.

Example

```
password-protected-zip
```

Syntax

```
no password-protected-zip
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable restricting transfer of password-protected ZIP files for the specified protocols.

Example

```
no password-protected-zip
```

Syntax

```
ms-office-macros
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable restricting transfer of MS-Office type files containing macros (VBA 5 and above).

Example

```
ms-office-macros
```

Syntax

```
no ms-office-macros
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable restricting transfer of MS-Office type files containing macros (VBA 5 and above) for the specified protocols.

Example

```
no ms-office-macros
```

Syntax

```
packed-executables
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable restricting transfer of packed executable files (UPX, FSG, etc.).

Example

```
restrict packed-executables http
```

Syntax

no packed-executables

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable restricting transfer of packed executable files (UPX, FSG, etc.) for the specified protocols.

Example

no packed-executables http

Syntax

smtp-responses

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable SMTP responses.

Example

smtp-responses

Syntax

no smtp-responses

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable SMTP responses.

Example

no smtp-responses

Syntax

eicar-detection

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable detection of EICAR test virus.

Example

eicar-detection

Syntax

no eicar-detection

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable detection of EICAR test virus.

Example

no eicar-detection

Syntax

http-byte-range

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable HTTP Byte-Range requests with Gateway AV.

Example

http-byte-range

Syntax

no http-byte-range

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable HTTP Byte-Range requests with Gateway AV.

Example

no http-byte-range

Syntax

ftp-rest

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Enable FTP 'REST' requests with Gateway AV.

Example

ftp-rest

Syntax

no ftp-rest

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Disable FTP 'REST' requests with Gateway AV.

Example

```
no ftp-rest
```

Syntax

```
scan-high-compression
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Scan parts of files with high compression ratios.

Example

```
scan-high-compression
```

Syntax

```
no scan-high-compression
```

Mode

Global Anti-Virus Prevention Profile for zone mode

Description

Do not scan parts of files with high compression ratios.

Example

```
no scan-high-compression
```

Syntax

```
no block-page <BLOCK_PAGE_NAME>
```

Mode

Config

Description

Delete a block page.

Options

<BLOCK_PAGE_NAME> Block page name.
Example: `\ "Corp Block Page\"`

Example

```
no block-page "Corp Block Page"
```

Syntax

no block-pages

Mode

Config

Description

Delete all block pages.

Example

no block-pages

Syntax

block-page <BLOCK_PAGE_NAME>

Mode

Config

Description

Add/edit block page and enter configuration mode.

Options

<BLOCK_PAGE_NAME> Block page name.
Example: \ "Corp Block Page\"

Example

block-page "Corp Block Page"

Syntax

name <BLOCK_PAGE_NAME>

Mode

Block Page

Description

Set block page name.

Options

<BLOCK_PAGE_NAME> Block page name.
Example: \ "Corp Block Page\"

Example

name "Corp Block Page"

Syntax

block-details

Mode

Block Page

Description

Enable inclusion of policy block details.

Example

block-details

Syntax

no block-details

Mode

Block Page

Description

Disable inclusion of policy block block-details.

Example

no block-details

Syntax

alert-text <WORD>

Mode

Block Page

Description

Set the block-page alert text.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

alert-text "This site had been blocked by the network administrator"

Syntax

no alert-text

Mode

Block Page

Description

Disable the block page alert text.

Example

no alert-text

Syntax

logo-icon { *data* <BLOCK_PAGE_LOGO_ICON_DATA> | *ftp* <FTP_URL> | *scp* <SCP_URL> }

Mode

Block Page

Description

Set/Upload the block page Base64 encoded logo icon.

Options

<i>data</i>	Set the block page base64 encoded logo icon data.
<i><BLOCK_PAGE_LOGO_ICON_DATA></i>	Block page logo icon data. Example: <i>data:image/gif;base64,BLOCKPAGE/BLOCKPAGELOGOICONDATA</i>
<i>ftp</i>	Set base64 encoded logo icon data using the FTP protocol.
<i><FTP_URL></i>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
<i>scp</i>	Set base64 encoded logo icon data using the SCP protocol.
<i><SCP_URL></i>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>

Example

```
logo-icon data "data:image/gif;base64,base64 encoded text goes here"
```

Syntax

```
no application-group [ uuid ] <APP_GROUP_NAME>
```

Mode

Config

Description

Delete a application group.

Options

<i>uuid</i>	Delete a application group by UUID.
<i><APP_GROUP_NAME></i>	Atom Object name. Example: <i>Application Tech Apps</i>

Example

```
no application-group "Denied Corp Applications"
```

Syntax

```
no application-groups
```

Mode

Config

Description

Delete all custom application groups.

Example

```
no application-groups
```

Syntax

```
application-group [ uuid ] <APP_GROUP_NAME>
```

Mode

Config

Description

Add/edit application group and enter configuration mode.

Options

<code>uuid</code>	Edit a application group by UUID.
<code><APP_GROUP_NAME></code>	Atom Object name. Example: <i>Application Tech Apps</i>

Example

`application-group "Denied Corp Applications"`

Syntax

`name <APP_GROUP_NAME>`

Mode

Application Group

Description

Set application group name.

Options

<code><APP_GROUP_NAME></code>	Atom Object name. Example: <i>Application Tech Apps</i>

Example

`name "Denied Corp Applications"`

Syntax

`uuid <UUID>`

Mode

Application Group

Description

Set application group UUID.

Options

<code><UUID></code>	Universally Unique Identifier (UUID). Min: 36 Max: 36 Example: <i>138a224d-c4c7-d621-0a00-c0eae49ce84c</i>

Example

`uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c`

Syntax

`no uuid`

Mode

Application Group

Description

Clear application group UUID.

Example

`no uuid`

Syntax

no application <APP_OBJECT_NAME>

Mode

Application Group

Description

Remove application from group.

Options

<APP_OBJECT_NAME> Atom Object name.
Example: *To Client App Group*

Example

no application "Google Picasa"

Syntax

no applications

Mode

Application Group

Description

Remove all applications from group.

Example

no applications

Syntax

application <APP_OBJECT_NAME>

Mode

Application Group

Description

Assign application to group.

Options

<APP_OBJECT_NAME> Atom Object name.
Example: *To Client App Group*

Example

application "Google Picasa"

Syntax

no application-group <APP_GROUP_NAME>

Mode

Application Group

Description

Remove application group from group.

Options

<APP_GROUP_NAME> Atom Object name.
Example: *Application Tech Apps*

Example

no application-group "Google Picasa"

Syntax

no application-groups

Mode

Application Group

Description

Remove all application group from group.

Example

no application-groups

Syntax

application-group <APP_GROUP_NAME>

Mode

Application Group

Description

Assign application group to group.

Options

<APP_GROUP_NAME> Atom Object name.
Example: *Application Tech Apps*

Example

application-group "Allowed US Applications"

Syntax

no reporting-profile [uuid] <REPORTING_PROFILE_NAME>

Mode

Config

Description

Delete a reporting profile.

Options

uuid Delete a reporting profile by UUID.
<REPORTING_PROFILE_NAME> Reporting profile name.
Example: *MyReportingProfile*

Example

```
no reporting-profile "Corp Reporting Profile"
```

Syntax

```
no reporting-profiles
```

Mode

Config

Description

Delete all reporting profiles.

Example

```
no reporting-profiles
```

Syntax

```
reporting-profile [ uuid ] <REPORTING_PROFILE_NAME>
```

Mode

Config

Description

Add/edit reporting profile and enter configuration mode.

Options

- uuid** Edit a reporting profile by UUID.
- <REPORTING_PROFILE_NAME>** Reporting profile name.
Example: *MyReportingProfile*

Example

```
reporting-profile "Corp Reporting Profile"
```

Syntax

```
clone reporting-profile [ uuid ] <REPORTING_PROFILE_NAME> [ new-name <WORD> ]
```

Mode

Config

Description

Clone reporting profile and enter configuration mode.

Options

- uuid** Clone a reporting profile by UUID.
- <REPORTING_PROFILE_NAME>** Reporting profile name.
Example: *MyReportingProfile*
- new-name** Clone a reporting profile with a new name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
clone reporting-profile "Corp Reporting Profile"
```

Syntax

name <REPORTING_PROFILE_NAME>

Mode

Reporting Profile

Description

Set reporting profile name.

Options

<REPORTING_PROFILE_NAME> Reporting profile name.
Example: *MyReportingProfile*

Example

name "Corp Reporting profile"

Syntax

uuid <UUID>

Mode

Reporting Profile

Description

Set reporting profile UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: *138a224d-c4c7-d621-0a00-c0eae49ce84c*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Reporting Profile

Description

Clear reporting profile UUID.

Example

no uuid

Syntax

frequency <UINT32>

Mode

Reporting Profile

Description

Set the frequency filter interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

frequency 60

Syntax

no frequency

Mode

Reporting Profile

Description

Clear the frequency filter interval.

Example

no frequency

Syntax

log-monitor

Mode

Reporting Profile

Description

Enable display in Log Monitor.

Example

log-monitor

Syntax

no log-monitor

Mode

Reporting Profile

Description

Disable display in log monitor.

Example

no log-monitor

Syntax

email-alert

Mode

Reporting Profile

Description

Enable email alert.

Example

```
email-alert
```

Syntax

```
no email-alert
```

Mode

Reporting Profile

Description

Disable email alert.

Example

```
no email-alert
```

Syntax

```
email-address <EMAIL>
```

Mode

Reporting Profile

Description

Set the email address to send alerts to.

Options

<EMAIL> E-mail in the form: aaaaa@bbb.com.
Example: *support@sonicwall.com*

Example

```
email-address
```

Syntax

```
no email-address
```

Mode

Reporting Profile

Description

Disable email alert.

Example

```
no email-address
```

Syntax

```
syslog
```

Mode

Reporting Profile

Description

Enable report events via syslog.

Example

```
syslog
```

Syntax

```
no syslog
```

Mode

Reporting Profile

Description

Disable report events via syslog.

Example

```
no syslog
```

Syntax

```
syslog-profile <UINT32>
```

Mode

Reporting Profile

Description

Set syslog profile.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
syslog-profile 1
```

Syntax

```
no syslog-profile
```

Mode

Reporting Profile

Description

Clear syslog profile.

Example

```
no syslog-profile
```

Syntax

```
ipfix
```

Mode

Reporting Profile

Description

Enable reporting of events via ipfix.

Example

ipfix

Syntax

no ipfix

Mode

Reporting Profile

Description

Disable reporting of events via ipfix.

Example

no ipfix

Syntax

color { black | blue | green | hex <HEX_UINT32> | orange | purple | red | rgb <UINT8> <UINT8> <UINT8> | yellow }

Mode

Reporting Profile

Description

Set the color to be displayed in the log monitor.

Options

<i>black</i>	Black.
<i>blue</i>	Blue.
<i>green</i>	Green.
<i>hex</i> <i><HEX_UINT32></i>	Hex representation. Hexadecimal integer in the form: 0xHHHHHHHH. Example: <i>0xaa55aa55</i>
<i>orange</i>	Orange.
<i>purple</i>	Purple.
<i>red</i>	Red.
<i>rgb</i> <i><UINT8></i>	Red, green, blue scale. Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>yellow</i>	Yellow.

Example

```
color black
color hex 0x00111333
color rgb 3 5 7
```

Syntax

```
event matched
```

Mode

Reporting Profile

Description

Enable report matched event.

Example

```
event matched
```

Syntax

```
no event matched
```

Mode

Reporting Profile

Description

Disable report matched event.

Example

```
no event matched
```

Syntax

```
event begin
```

Mode

Reporting Profile

Description

Enable report event begin.

Example

```
event begin
```

Syntax

```
no event begin
```

Mode

Reporting Profile

Description

Disable report event begin .

Example

no event begin

Syntax

event end

Mode

Reporting Profile

Description

Enable report end event.

Example

event end

Syntax

no event end

Mode

Reporting Profile

Description

Disable report event end .

Example

no event end

Syntax

no dos-action-profile [uuid] <DOS_ACTION_PROFILE_NAME>

Mode

Config

Description

Delete DoS action profile.

Options

<i>uuid</i>	Delete a DoS action profile by UUID.
<i><DOS_ACTION_PROFILE_NAME></i>	Dos action profile name. Example: <i>Office DoS Action Profile</i>

Example

no dos-action-profile "Office DoS Action Profile"

Syntax

no dos-action-profiles

Mode

Config

Description

Delete all DoS action profiles.

Example

```
no dos-action-profiles
```

Syntax

```
dos-action-profile [ uuid ] <DOS_ACTION_PROFILE_NAME>
```

Mode

Config

Description

Add/Edit DoS action profile and enter configuration mode.

Options

uuid	Add/Edit a DoS action profile by UUID.
<DOS_ACTION_PROFILE_NAME>	Dos action profile name. Example: <i>Office DoS Action Profile</i>

Example

```
dos-action-profile "Office DoS Action Profile"
```

Syntax

```
clone dos-action-profile [ uuid ] <DOS_ACTION_PROFILE_NAME> [ new-name <WORD> ]
```

Mode

Config

Description

Clone DoS action profile.

Options

uuid	Clone a DoS action profile by UUID.
<DOS_ACTION_PROFILE_NAME>	Dos action profile name. Example: <i>Office DoS Action Profile</i>
new-name	Clone Dos action profile with a new name.
<WORD>	Word in the form: WORD or "QUOTED STRING". Example: <i>abc</i>

Example

```
clone dos-action-profile "Office DoS Action Profile"
```

Syntax

```
uuid <DOS_ACTION_PROFILE_UUID>
```

Mode

DoS Action Profile

Description

DoS action profile UUID.

Options

<DOS_ACTION_PROFILE_UUID>	DOS action profile UUID. Example: <i>7df86117-0a7c-f329-3400-2cb8ed3d8a10</i>

Example

```
uuid 7df86117-0a7c-f329-3400-2cb8ed3d8a10
```

Syntax

```
no uuid
```

Mode

DoS Action Profile

Description

DoS action profile UUID.

Example

```
no uuid
```

Syntax

```
name <DOS_ACTION_PROFILE_NAME>
```

Mode

DoS Action Profile

Description

DoS action profile name.

Options

<DOS_ACTION_PROFILE_NAME> Dos action profile name.
Example: *Office DoS Action Profile*

Example

```
name "Office DoS Action Profile"
```

Syntax

```
no name
```

Mode

DoS Action Profile

Description

Clear DoS action profile name.

Example

```
no name
```

Syntax

```
syn-flood-protection enable
```

Mode

DoS Action Profile

Description

Enable SYN Flood Protection.

Example

```
syn-flood-protection enable
```

Syntax

```
no syn-flood-protection enable
```

Mode

DoS Action Profile

Description

Disable SYN Flood Protection.

Example

```
no syn-flood-protection enable
```

Syntax

```
syn-flood-protection mode { always-proxy | proxy-suspect-attack | watch-and-report }
```

Mode

DoS Action Profile

Description

Set TCP SYN flood protection mode.

Options

<i>always-proxy</i>	Always proxy WAN client connections.
<i>proxy-suspect-attack</i>	Proxy WAN client connections when attack is suspected.
<i>watch-and-report</i>	Watch and report possible SYN floods.

Example

```
syn-flood-protection mode watch-and-report
```

Syntax

```
syn-attack-threshold <UINT32>
```

Mode

DoS Action Profile

Description

Set SYN attack threshold (incomplete connection attempts / second).

Options

- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
syn-attack-threshold 300
```

Syntax

no syn-attack-threshold

Mode

DoS Action Profile

Description

Clear SYN attack threshold (incomplete connection attempts / second).

Example

no syn-attack-threshold

Syntax

tcp-sack

Mode

DoS Action Profile

Description

Enable TCP SACK option support.

Example

tcp-sack

Syntax

no tcp-sack

Mode

DoS Action Profile

Description

Disable TCP SACK option support.

Example

no tcp-sack

Syntax

limit-mss [enable | max <UINT16>]

Mode

DoS Action Profile

Description

Enable limit MSS sent (when connections are proxied).

Options

enable Enable limit MSS sent (when connections are proxied).

max Set maximum TCP MSS sent to WAN clients.

<UINT16> Integer in the form: D OR 0xHHHH.

Example: 123

Example

```
limit-mss max 1460
```

Syntax

```
no limit-mss [ enable ]
```

Mode

DoS Action Profile

Description

Disable limit MSS sent (when connections are proxied).

Options

enable Disable limit MSS sent (when connections are proxied).

Example

```
no limit-mss
```

Syntax

```
log-syn-packets
```

Mode

DoS Action Profile

Description

Enable always log SYN packets received.

Example

```
log-syn-packets
```

Syntax

```
no log-syn-packets
```

Mode

DoS Action Profile

Description

Disable always log SYN packets received.

Example

```
no log-syn-packets
```

Syntax

```
syn-flood-blacklisting
```

Mode

DoS Action Profile

Description

Enable SYN/RST/FIN flood blacklisting.

Example

```
syn-flood-blacklisting
```

Syntax

```
no syn-flood-blacklisting
```

Mode

DoS Action Profile

Description

Disable SYN/RST/FIN flood blacklisting.

Example

```
no syn-flood-blacklisting
```

Syntax

```
blacklist-threshold <UINT32>
```

Mode

DoS Action Profile

Description

Set threshold for SYN/RST/FIN flood blacklisting (packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
blacklist-threshold 1000
```

Syntax

```
never-blacklist-wan
```

Mode

DoS Action Profile

Description

Enable never blacklist WAN machines.

Example

```
never-blacklist-wan
```

Syntax

```
no never-blacklist-wan
```

Mode

DoS Action Profile

Description

Disable never blacklist WAN machines.

Example

```
no never-never-blacklist-wan
```

Syntax

```
management
```

Mode

DoS Action Profile

Description

Enable always allow SonicWall management traffic.

Example

```
management
```

Syntax

```
no management
```

Mode

DoS Action Profile

Description

Disable always allow SonicWall management traffic.

Example

```
management
```

Syntax

```
udp-flood-protection
```

Mode

DoS Action Profile

Description

Enable UDP flood protection.

Example

```
udp-flood-protection
```

Syntax

```
no udp-flood-protection
```

Mode

DoS Action Profile

Description

Disable UDP flood protection.

Example

```
no udp-flood-protection
```

Syntax

```
udp-flood-attack threshold <UINT32>
```

Mode

DoS Action Profile

Description

Set UDP flood attack threshold (UDP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
udp-flood-attack threshold 1000
```

Syntax

```
no udp-flood-attack threshold
```

Mode

DoS Action Profile

Description

Clear UDP flood attack threshold (UDP packets / sec).

Example

```
no udp-flood-attack threshold
```

Syntax

```
udp-flood-attack block-timeout <UINT8>
```

Mode

DoS Action Profile

Description

Set UDP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
udp-flood-attack block-timeout 2
```

Syntax

```
no udp-flood-attack block-timeout
```

Mode

DoS Action Profile

Description

Clear UDP flood attack blocking time (sec).

Example

```
no udp-flood-attack block-timeout
```

Syntax

```
icmp-flood-protection
```

Mode

DoS Action Profile

Description

Enable ICMP flood protection.

Example

```
icmp-flood-protection
```

Syntax

```
no icmp-flood-protection
```

Mode

DoS Action Profile

Description

Disable ICMP flood protection.

Example

```
no icmp-flood-protection
```

Syntax

```
icmp-flood-attack threshold <UINT32>
```

Mode

DoS Action Profile

Description

Set ICMP flood attack threshold (ICMP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
icmp-flood-attack threshold 1000
```

Syntax

```
no icmp-flood-attack threshold
```

Mode

DoS Action Profile

Description

Clear ICMP flood attack threshold (ICMP packets / sec).

Example

```
no icmp-flood-attack threshold 1000
```

Syntax

```
icmp-flood-attack block-timeout <UINT8>
```

Mode

DoS Action Profile

Description

Set ICMP flood attack blocking time (sec).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
icmp-flood-attack block-timeout 2
```

Syntax

```
no icmp-flood-attack block-timeout
```

Mode

DoS Action Profile

Description

Clear ICMP flood attack blocking time (sec).

Example

```
no icmp-flood-attack block-timeout 2
```

Syntax

```
ddos protection
```

Mode

DoS Action Profile

Description

Enable DDoS Protection.

Example

```
ddos protection
```

Syntax

no ddos protection

Mode

DoS Action Profile

Description

Disable DDoS Protection.

Example

no ddos protection

Syntax

ddos threshold <UINT32>

Mode

DoS Action Profile

Description

Set threshold for WAN DDOS protection (non-TCP packets / sec).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

ddos threshold 1000

Syntax

no ddos threshold

Mode

DoS Action Profile

Description

Clear threshold for WAN DDOS protection.

Example

no ddos threshold

Syntax

ddos fliter-bypass-rate <UINT32>

Mode

DoS Action Profile

Description

Set WAN DDOS filter bypass rate (every n packets).

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
ddos fliter-bypass-rate 100
```

Syntax

```
no ddos fliter-bypass-rate
```

Mode

DoS Action Profile

Description

Clear WAN DDOS filter bypass rate.

Example

```
no ddos fliter-bypass-rate
```

Syntax

```
ddos allow-list-timeout <UINT32>
```

Mode

DoS Action Profile

Description

Set WAN DDOS allow list timeout.

Options

- <UINT32>** Integer in the form: D OR 0xHHHHHHHH. Example: 123

Example

```
ddos allow-list-timeout 100
```

Syntax

```
no ddos allow-list-timeout
```

Mode

DoS Action Profile

Description

Clear WAN DDOS allow list timeout.

Example

```
no ddos allow-list-timeout
```

Syntax

```
ddos on-wan-interfaces
```

Mode

DoS Action Profile

Description

Enable DDOS protection on WAN interfaces.

Example

```
ddos on-wan-interfaces
```

Syntax

```
no ddos on-wan-interfaces
```

Mode

DoS Action Profile

Description

Disable DDOS protection on WAN interfaces.

Example

```
no ddos on-wan-interfaces
```

Syntax

```
ddos management
```

Mode

DoS Action Profile

Description

Enable always allow SonicWall management traffic (non-tcp floods).

Example

```
ddos management
```

Syntax

```
no ddos management
```

Mode

DoS Action Profile

Description

Disable always allow SonicWall management traffic (non-tcp floods).

Example

```
no ddos management
```

Syntax

```
spank-protection
```

Mode

DoS Action Profile

Description

Enable spank protectionn.

Example

spank-protection

Syntax

no spank-protection

Mode

DoS Action Profile

Description

Disable spank protection.

Example

no spank-protection

Syntax

smurf-protection

Mode

DoS Action Profile

Description

Enable smurf protectionn.

Example

smurf-protection

Syntax

no smurf-protection

Mode

DoS Action Profile

Description

Disable smurf protection.

Example

no smurf-protection

Syntax

land-attack-protection

Mode

DoS Action Profile

Description

Enable land attack protection.

Example

land-attack-protection

Syntax

no land-attack-protection

Mode

DoS Action Profile

Description

Disable land attack protection.

Example

no land-attack-protection

Syntax

connection-limit enable

Mode

DoS Action Profile

Description

Enable connection limiting.

Example

connection-limit enable

Syntax

no connection-limit enable

Mode

DoS Action Profile

Description

Disable connection limiting.

Example

no connection-limit enable

Syntax

connection-limit maximum <UINT8>

Mode

DoS Action Profile

Description

Number of connections allowed (% of maximum connections).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

connection-limit maximum 20

Syntax

```
connection-limit destination [ enable | threshold <UINT16> ]
```

Mode

DoS Action Profile

Description

Enable connection limit for each destination IP address.

Options

<i>enable</i>	Enable connection limit for each destination IP address.
<i>threshold</i>	Set the destination IP address connection limit threshold.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
connection-limit destination threshold 128
```

Syntax

```
no connection-limit destination [ enable | threshold ]
```

Mode

DoS Action Profile

Description

Disable connection limit for each destination IP address.

Options

<i>enable</i>	Disable connection limit for each destination IP address.
<i>threshold</i>	Clear the destination IP address connection limit threshold.

Example

```
no connection-limit destination
```

Syntax

```
connection-limit source [ enable | threshold <UINT16> ]
```

Mode

DoS Action Profile

Description

Enable connection limit for each source IP address.

Options

<i>enable</i>	Enable connection limit for each source IP address.
<i>threshold</i>	Set the source IP address connection limit threshold.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

connection-limit source threshold 128

Syntax

no connection-limit source [enable | threshold]

Mode

DoS Action Profile

Description

Disable connection limit for each source IP address.

Options

enable Disable connection limit for each source IP address.

threshold Clear the source IP address connection limit threshold.

Example

no connection-limit source

Syntax

no custom-match <CUSTOM_MATCH_NAME>

Mode

Config

Description

Delete a custom match object.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no custom-match "FTP Client Download Match"

Syntax

no custom-matches

Mode

Config

Description

Delete all custom match objects.

Example

no custom-matches

Syntax

custom-match <CUSTOM_MATCH_NAME>

Mode

Config

Description

Add/edit custom match and enter configuration mode.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

custom match "FTP Client Download Match"

Syntax

clone custom-match <CUSTOM_MATCH_NAME> [new-name <WORD>]

Mode

Config

Description

Clone custom match object.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

new-name Clone custom match object with a new name.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

clone custom-match "FTP Client Download Match"

Syntax

no custom-match-group [uuid] <CUSTOM_MATCH_GROUP_NAME>

Mode

Config

Description

Delete a custom match group.

Options

uuid Delete a custom match group by UUID.

<CUSTOM_MATCH_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no custom-match-group uuid 00000000-0000-0002-1b00-2cb8ed3d8a10

Syntax

no custom-match-groups

Mode

Config

Description

Delete all custom match groups.

Example

no custom match-groups

Syntax

custom-match-group [uuid] <CUSTOM_MATCH_GROUP_NAME>

Mode

Config

Description

Add/edit custom match group and enter configuration mode.

Options

- uuid** Edit a custom match group by UUID.
- <CUSTOM_MATCH_GROUP_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

custom-match-group uuid 00000000-0000-0002-1b00-2cb8ed3d8a10

Syntax

clone custom-match-group [uuid] <CUSTOM_MATCH_GROUP_NAME> [new-name <WORD>]

Mode

Config

Description

Clone custom match group.

Options

- uuid** Clone a custom match group by UUID.
- <CUSTOM_MATCH_GROUP_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- new-name** Clone custom match group with a new name.
- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

clone custom-match-group customMatchGrp
clone custom-match-group uuid 00000000-0000-0002-1b00-2cb8ed3d8a10

Syntax

name <CUSTOM_MATCH_GROUP_NAME>

Mode

Custom Match Group

Description

Custom match group name.

Options

<CUSTOM_MATCH_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

name "Email Content Match Group"

Syntax

no name

Mode

Custom Match Group

Description

Clear Custom match group name.

Example

no name

Syntax

uuid <CUSTOM_MATCH_GROUP_UUID>

Mode

Custom Match Group

Description

Set custom match group UUID.

Options

<CUSTOM_MATCH_GROUP_UUID> Custom match group UUID.
Example: *7df86117-0a7c-f329-3400-2cb8ed3d8a10*

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Custom Match Group

Description

Clear custom match group UUID.

Example

no uuid

Syntax

no custom-match <CUSTOM_MATCH_NAME>

Mode

Custom Match Group

Description

Delete specified custom match.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

no custom-match "Sensitive Email Download"

Syntax

no custom-matches

Mode

Custom Match Group

Description

Delete all custom matches.

Example

no custom-matches

Syntax

custom-match <CUSTOM_MATCH_NAME>

Mode

Custom Match Group

Description

Add specified custom match.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

custom-match "Deny Sensitive Download"

Syntax

no custom-match-group <CUSTOM_MATCH_GROUP_NAME>

Mode

Custom Match Group

Description

Delete specified custom match group.

Options

<CUSTOM_MATCH_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
no custom-match-group "Email Content Group"
```

Syntax

```
no custom-match-groups
```

Mode

Custom Match Group

Description

Delete all custom match groups.

Example

```
no custom-match-groups
```

Syntax

```
custom-match-group <CUSTOM_MATCH_GROUP_NAME>
```

Mode

Custom Match Group

Description

Add specified custom match group.

Options

<CUSTOM_MATCH_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
custom-match-group "Email Content Group"
```

Syntax

```
name <CUSTOM_MATCH_NAME>
```

Mode

Custom Match

Description

Custom match name.

Options

<CUSTOM_MATCH_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name "Sensitive Email Content"
```

Syntax

```
no name
```

Mode

Custom Match

Description

Clear custom match name.

Example

no name

Syntax

uuid <UUID>

Mode

Custom Match

Description

Set custom match UUID.

Options

<UUID> Universally Unique Identifier (UUID).
Min: 36
Max: 36
Example: 138a224d-c4c7-d621-0a00-c0eae49ce84c

Example

uuid f40b27d6-b8b9-a4fc-0300-c0eae49ce84c

Syntax

no uuid

Mode

Custom Match

Description

Clear custom match UUID.

Example

no uuid

Syntax

type { app-control | custom | ftp { { client | client-download | client-upload | data-transfer } } | http { { client | server } } | ips | pop3 { { client | server } } | smtp-client }

Mode

Custom Match

Description

Set custom match type.

Options

app-control Custom match type App Control Content.
custom Custom match type custom.

<i>ftp</i>	FTP.
<i>client</i>	FTP client.
<i>client-download</i>	FTP client file download.
<i>client-upload</i>	FTP client file upload.
<i>data-transfer</i>	FTP data transfer.
<i>http</i>	HTTP.
<i>client</i>	HTTP client.
<i>server</i>	HTTP server.
<i>ips</i>	Custom match type IPS Content.
<i>pop3</i>	POP3.
<i>client</i>	Pop3 client.
<i>server</i>	Pop3 server.
<i>smtp-client</i>	SMTP client.

Example

```
type http client
```

Syntax

```
match-object { excluded <CUSTOM_MATCH_MATCH_OBJECT> | included <CUSTOM_MATCH_MATCH_OBJECT> | object
<CUSTOM_MATCH_MATCH_OBJECT> }
```

Mode

Custom Match

Description

Set match object for this custom match.

Options

<i>excluded</i>	Exclude match object.
<i><CUSTOM_MATCH_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>included</i>	Include match object.
<i><CUSTOM_MATCH_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>object</i>	Include match object.
<i><CUSTOM_MATCH_MATCH_OBJECT></i>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
match-object object "mpg extension"
```

Syntax

```
mail-from included <CUSTOM_MATCH_EMAIL_OBJECT>
```

Mode

Custom Match

Description

Set the included from e-mail object for the custom match.

Options

<CUSTOM_MATCH_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

mail-from included any mail-from included "John Doe"

Syntax

mail-from excluded <CUSTOM_MATCH_EMAIL_OBJECT>

Mode

Custom Match

Description

Set the excluded from e-mail object for the custom match.

Options

<CUSTOM_MATCH_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

mail-from excluded "Jane Doe"

Syntax

no mail-from excluded

Mode

Custom Match

Description

Clear the excluded from e-mail object for the custom match.

Options

excluded Clear the excluded from e-mail object for the custom match.

Example

no mail-from excluded

Syntax

rcpt-to included <CUSTOM_MATCH_EMAIL_OBJECT>

Mode

Custom Match

Description

Set the included RCPT to e-mail address object for the custom match.

Options

<CUSTOM_MATCH_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

rcpt-to included any rcpt-to included "John Doe"

Syntax

rcpt-to excluded <CUSTOM_MATCH_EMAIL_OBJECT>

Mode

Custom Match

Description

Set the excluded RCPT to e-mail address object for the custom match.

Options

<CUSTOM_MATCH_EMAIL_OBJECT> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

rcpt-to excluded "Jane Doe"

Syntax

no rcpt-to excluded

Mode

Custom Match

Description

Clear the excluded RCPT to e-mail object for the custom match.

Options

excluded Clear the excluded RCPT to e-mail object for the custom match.

Example

no rcpt-to excluded

Syntax

connection-side { both | client | server }

Mode

Custom Match

Description

Set connection side.

Options

both Both sides.

client Client side.

server Server side.

Example

`connection-side server`

Syntax

`direction { advanced [ [ from { any | zone <CUSTOM_MATCH_ZONE> } ] ] [ [ to { any | zone <CUSTOM_MATCH_ZONE> } ] ] | basic [ [ both | incoming | outgoing ] ] }`

Mode

Custom Match

Description

Set direction.

Options

advanced	Advanced.
from	From.
any	From any zone.
zone	Set the source zone.
<CUSTOM_MATCH_ZONE>	Zone object name. Example: <i>DMZ</i>
to	To.
any	To any zone.
zone	Set the destination zone.
<CUSTOM_MATCH_ZONE>	Zone object name. Example: <i>DMZ</i>
basic	Basic.
both	Both directions.
incoming	Incoming.
outgoing	Outgoing.

Example

`direction incoming`

Syntax

`show security-action-profiles [ { custom | default } ] [ { pending-config | with-pending-config } ]`

Mode

All Modes

Description

Show all security action profiles.

Options

custom	Show custom configuration.

default	Show system/factory default configuration.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show security-action-profiles
show security-action-profiles pattern per-action
show security-action-profiles unused
```

Syntax

```
show security-action-profile [ uuid ] <SECURITY_ACTION_PROFILE_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show security action profile.

Options

uuid	Show a security action profile by UUID.
<SECURITY_ACTION_PROFILE_NAME>	Security action profile name. Example: <i>MySecurityActionProfile</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show security-action-profile "Corp Security Action Profile"
```

Syntax

```
show dos-policies [ uuid <DOS_POLICY_UUID> ] [ name <DOS_POLICY_NAME> ] [ counter-status | counters | statistics ] [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all DoS policies.

Options

uuid	Show a DoS Policy by UUID.
<DOS_POLICY_UUID>	DOS policy UUID. Example: <i>00000000-0000-0004-1d00-2cb8ed3d8a10</i>
name	Show a DoS Policy by name.
<DOS_POLICY_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
counter-status	Show counter status for all DoS Policies.
counters	Show counter statistics for all DoS Policies.
statistics	Show statistics for all DoS Policies.
custom	Show custom configuration.
default	Show system/factory default configuration.

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show dos-policies
show dos-policies pattern WAN
show dos-policies unused
```

Syntax

```
show dos-policy uuid <DOS_POLICY_UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show DoS Policy.

Options

- <DOS_POLICY_UUID>*** DOS policy UUID.
Example: *00000000-0000-0004-1d00-2cb8ed3d8a10*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

```
show dos-policy uuid 00000000-0000-0004-1d00-2cb8ed3d8a10
```

Syntax

```
show website-objects
```

Mode

All Modes

Description

Show all website objects.

Example

```
show website-objects
```

Syntax

```
show website-object [ uuid ] <WEB_SITE_OBJ_NAME>
```

Mode

All Modes

Description

Show website object.

Options

- uuid*** Show a website object by UUID.
- <WEB_SITE_OBJ_NAME>*** Website object name.

Example: *Website domain object*

Example

```
show website-object "Object Name"
```

Syntax

```
show website-groups
```

Mode

All Modes

Description

Show all website groups.

Example

```
show website-groups
```

Syntax

```
show website-group [ uuid ] <WEB_SITE_GRP_NAME>
```

Mode

All Modes

Description

Show website group.

Options

uuid	Show a website group by UUID.
<WEB_SITE_GRP_NAME>	Website group name. Example: <i>Website domain group</i>

Example

```
show website-group "Group Name"
```

Syntax

```
show decryption-policies [ { client | server | ssh } ] [ statistics ] [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all decryption policies.

Options

client	Show client decryption policies.
server	Show server decryption policies.
ssh	Show ssh decryption policies.
statistics	Show statistics for all decryption policies.
custom	Show custom configuration.

default	Show system/factory default configuration.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show decryption-policies
show decryption-policies pattern WAN
show decryption-policies unused
```

Syntax

```
show decryption-policy { client | server | ssh } { name <DEC_POLICY_NAME> | uuid <DEC_POLICY_UUID> } [ statistics ] [ {
pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show decryption policy.

Options

client	Show client decryption policies.
server	Show server decryption policies.
ssh	Show ssh decryption policies.
name	name.
<DEC_POLICY_NAME>	Decryption policy name. Example: <i>decPolicy1</i>
uuid	Show a decryption policy by UUID.
<DEC_POLICY_UUID>	Universally Unique Identifier (UUID). Example: <i>550e8400-e29b-41d4-a716-446655440000</i>
statistics	Show statistics for specified decryption policy.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show decryption-policy "Corp Decryption Policy"
```

Syntax

```
show countries [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all countries.

Options

pending-config	Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show countries

Syntax

show country [uuid] <COUNTRY_OBJECT_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show country.

Options

- uuid*** Show a country object by UUID.
- <COUNTRY_OBJECT_NAME>*** Word in the form: WORD or \"QUOTED STRING\".
Example: *China*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show country "Ireland"

Syntax

show country-groups [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all country groups.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show country-groups

Syntax

show country-group [uuid] <COUNTRY_GROUP_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show country group.

Options

uuid	Show a country group by UUID.
<COUNTRY_GROUP_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>China</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show country-group "Middle East"
```

Syntax

```
show security-policies [ [ [ ipv4 | ipv6 ] [ from <SECURITY_POLICY_ZONE_NAME> to <SECURITY_POLICY_ZONE_NAME> | name
<SECURITY_POLICY_NAME> | unused | uuid <SECURITY_POLICY_UUID> ] [ statistics ] [ { pending-config | with-pending-config } ] ]
| max-count ]
```

Mode

All Modes

Description

Show all security policies.

Options

ipv4	Show IPv4 security policies.
ipv6	Show IPv6 security policies.
from	Source.
<SECURITY_POLICY_ZONE_NAME>	Security policy zone name. Example: <i>DMZ</i>
to	Destination.
<SECURITY_POLICY_ZONE_NAME>	Security policy zone name. Example: <i>DMZ</i>
name	Show a security policy by name.
<SECURITY_POLICY_NAME>	Security policy name. Example: <i>abc</i>
unused	Show access rules assigned to a Zone that has not been assigned to an interface.
uuid	Show a security policy by UUID.
<SECURITY_POLICY_UUID>	Security policy UUID. Example: <i>00000000-0000-0001-0700-2cb8ed4acd38</i>
statistics	Show statistics for all security Policies.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.
max-count	Show security policies max count.

Example

```
show security-policies ipv4
show security-policies ipv4 statistics
show security-policies ipv4 uuid 00000000-0000-0001-0700-2cb8ed4acd38 statistics
show security-policies max-count
```

Syntax

```
show security-policy ipv4 uuid <SECURITY_POLICY_UUID> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show security policy.

Options

- uuid**

Show a security policy by UUID.
- <SECURITY_POLICY_UUID>**

Security policy UUID.
Example: *00000000-0000-0001-0700-2cb8ed4acd38*
- pending-config**

Show pending configuration changes.
- with-pending-config**

View current configuration with pending changes included in the output.

Example

show security-policy uuid 00000000-0000-0001-0700-2cb8ed4acd38

Syntax

show security-policy ipv6 uuid <SECURITY_POLICY_UUID> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show security policy.

Options

- uuid**

Show a security policy by UUID.
- <SECURITY_POLICY_UUID>**

Security policy UUID.
Example: *00000000-0000-0001-0700-2cb8ed4acd38*
- pending-config**

Show pending configuration changes.
- with-pending-config**

View current configuration with pending changes included in the output.

Example

show security-policy uuid 00000000-0000-0001-0700-2cb8ed4acd38

Syntax

show policy { section uuid <POLICY_SECTION_UUID> name <POLICY_SECTION_NAME> | sections } [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show policy sections.

Options

- section**

Policy section.
- uuid**

Show a policy section by UUID.
- <POLICY_SECTION_UUID>**

Policy section UUID.
Example: *00000000-0000-0001-0700-2cb8ed4acd38*
- name**

Section name.
- <POLICY_SECTION_NAME>**

Policy section name.

	Example: <i>test</i>
<i>sections</i>	Policy sections.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

```
show policy sections
```

Syntax

```
show web-category-objects status
```

Mode

All Modes

Description

Show all web category objects.

Options

status Show url object status.

Example

```
show web-category-objects
```

Syntax

```
show web-category-groups [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all web category groups.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

```
show web-category-groups
```

Syntax

```
show web-category-group [ uuid ] <WEB_CATEGORY_GRP_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show web category group.

Options

uuid	Show a web category group by UUID.
<WEB_CATEGORY_GRP_NAME>	Web category group name. Example: <i>Web category group</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show web-category-group "Group Name"
```

Syntax

```
show threat-prevention-profiles [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all threat prevention profiles.

Options

pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show threat-prevention-profiles
```

Syntax

```
show threat-prevention-profile [ uuid ] <THREAT_PROFILE_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show threat prevention profile.

Options

uuid	Show a threat prevention profile by UUID.
<THREAT_PROFILE_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>DNS Category Profile</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show threat-prevention-profile "Threat Prevention Signature Profile"
```

Syntax

```
show policies-settings base [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show policies settings.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show policies-settings

Syntax

show block-pages [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all block pages.

Options

- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show block-pages

Syntax

show block-page <BLOCK_PAGE_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show block-page.

Options

- <BLOCK_PAGE_NAME>*** Block page name.
Example: *"Corp Block Page"*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show block-page "Corp Block Page"

Syntax

```
show application-groups [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all application groups.

Options

- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show application-groups
```

Syntax

```
show application-group [ uuid ] <APP_GROUP_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show application group.

Options

- uuid** Show a application group by UUID.
- <APP_GROUP_NAME>** Atom Object name.
Example: *Application Tech Apps*
- pending-config** Show pending configuration changes.
- with-pending-config** View current configuration with pending changes included in the output.

Example

```
show application-group "Allowed Corp Applications"
```

Syntax

```
show reporting-profiles [ { custom | default } ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all reporting profiles.

Options

- custom** Show custom configuration.
- default** Show system/factory default configuration.
- pending-config** Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show reporting-profiles

Syntax

show reporting-profile [uuid] <REPORTING_PROFILE_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show reporting-profile.

Options

- uuid*** Show reporting profile by UUID.
- <REPORTING_PROFILE_NAME>*** Reporting profile name.
Example: *MyReportingProfile*
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show reporting-profile "Corp Reporting Profile"

Syntax

show dos-action-profiles [unused | used] [pattern <WORD>] [statistics] [{ custom | default }] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all DoS action profiles.

Options

- unused*** Show unused DoS action profiles.
- used*** Show used DoS action profiles.
- pattern*** Show DoS action profiles that have the given pattern match.
<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*
- statistics*** Show statistics for all DoS action profiles.
- custom*** Show custom configuration.
- default*** Show system/factory default configuration.
- pending-config*** Show pending configuration changes.
- with-pending-config*** View current configuration with pending changes included in the output.

Example

show dos-action-profiles
show dos-action-profiles pattern deny
show dos-action-profiles unused

Syntax

```
show dos-action-profile [ uuid ] <DOS_ACTION_PROFILE_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show DoS action profile.

Options

uuid	Show a Dos action profile by UUID.
<DOS_ACTION_PROFILE_NAME>	Dos action profile name. Example: <i>Office DoS Action Profile</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show dos-action-profile "Corp DoS Action Profile"
```

Syntax

```
show custom-matches [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show all custom matches.

Options

pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show custom-matches
```

Syntax

```
show custom-match <CUSTOM_MATCH_NAME> [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show custom-match.

Options

<CUSTOM_MATCH_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
pending-config	Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show custom-match "FTP Download File Content"

Syntax

show custom-match-groups [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show all custom-match groups.

Options

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show custom-match-groups

Syntax

show custom-match-group [uuid] <CUSTOM_MATCH_GROUP_NAME> [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show custom match group.

Options

uuid Show a custom match group by UUID.
<CUSTOM_MATCH_GROUP_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

pending-config Show pending configuration changes.

with-pending-config View current configuration with pending changes included in the output.

Example

show custom-match-group "Web Content Match Group"
show custom-match-group uuid 00000000-0000-0002-1b00-2cb8ed3d8a10

Syntax

switch-controller

Mode

Config

Description

Enter Switch Controller mode.

Example

switch-controller

Syntax

port <WORD> switch <SWITCH_NAME>

Mode

Switch Controller

Description

Switch Controller Port Mode.

Options

- <WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
- switch Switch.
- <SWITCH_NAME> Switch Name.
Example: \"My Switch\"

Example

port

Syntax

clear-statistics switch <SWITCH_NAME>

Mode

Switch Controller

Description

Clear Switch Statistics.

Options

- <SWITCH_NAME> Switch Name.
Example: \"My Switch\"

Example

clear-statistics switch LANSwitch

Syntax

enable

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port.

Example

enable

Syntax

no enable

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port.

Example

no enable

Syntax

port-description <WORD>

Mode

Switch Controller Port Switch

Description

Set port description.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

port-description "mgmt port 7"

Syntax

no port-description

Mode

Switch Controller Port Switch

Description

Clear port description.

Example

no port-description

Syntax

link-speed { *auto-negotiate* | *full* { { *10* | *100* | *1000* | *10000* } } | *half* { { *10* | *100* } } }

Mode

Switch Controller Port Switch

Description

Configure port link speed.

Options

auto-negotiate Set port link speed to auto-negotiate

full Full duplex.

10	10 Mbps - Full Duplex
100	100 Mbps - Full Duplex
1000	1000 Mbps - Full Duplex
10000	10000 Mbps - Full Duplex
half	Half duplex.
10	10 Mbps - Half Duplex
100	100 Mbps - Half Duplex

Example

```
link-speed auto-negotiate
```

Syntax

```
stp
```

Mode

Switch Controller Port Switch

Description

Enable Stp_state for Port.

Example

```
stp
```

Syntax

```
no stp
```

Mode

Switch Controller Port Switch

Description

Disable Stp_state for Port.

Example

```
no stp
```

Syntax

```
poe
```

Mode

Switch Controller Port Switch

Description

Switch Controller Port POE Status.

Example

```
poe
```

Syntax

no poe

Mode

Switch Controller Port Switch

Description

Switch Controller Port POE Status.

Example

no poe

Syntax

portshield-uplink

Mode

Switch Controller Port Switch

Description

Enable dedicated uplink for port's portshield interface.

Example

portshield-uplink

Syntax

no portshield-uplink

Mode

Switch Controller Port Switch

Description

Disable dedicated uplink for port's portshield interface.

Example

no portshield-uplink

Syntax

portshield-uplink-secondary

Mode

Switch Controller Port Switch

Description

Enable secondary dedicated uplink for port's portshield interface.

Example

portshield-uplink-secondary

Syntax

```
no portshield-uplink-secondary
```

Mode

Switch Controller Port Switch

Description

Disable secondary dedicated uplink for port's portshield interface.

Example

```
no portshield-uplink-secondary
```

Syntax

```
poe-priority { critical | high | low | medium }
```

Mode

Switch Controller Port Switch

Description

Configure port POE power priority level.

Options

critical Critical

high High

low low

medium Medium

Example

```
poe-priority critical
```

Syntax

```
poe-limit-type { auto-class | user-defined }
```

Mode

Switch Controller Port Switch

Description

Configure port POE power limit type.

Options

auto-class Auto Class

user-defined User Defined

Example

```
poe-limit-type auto-class
```

Syntax

```
power-limit <UINT16>
```

Mode

Switch Controller Port Switch

Description

Configure port POE power limit.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
power-limit 10
```

Syntax

```
no power-limit
```

Mode

Switch Controller Port Switch

Description

Diabie port POE power limit.

Example

```
no power-limit
```

Syntax

```
port-isolation
```

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port Isolation.

Example

```
port-isolation
```

Syntax

```
no port-isolation
```

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port Isolation.

Example

```
no port-isolation
```

Syntax

```
voice-vlan
```

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port Voice VLAN state.

Example

```
voice-vlan
```

Syntax

```
no voice-vlan
```

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port Voice VLAN state.

Example

```
no voice-vlan
```

Syntax

```
voice-vlan-cos-mode { all | src }
```

Mode

Switch Controller Port Switch

Description

Configure Switch Controller Port Voice VLAN Cos mode.

Options

all All

src Source

Example

```
voice-vlan-cos-mode src
```

Syntax

```
cos-value <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Switch Controller QoS settings cos value.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

cos-value 5

Syntax

trust

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port QoS trust.

Example

trust

Syntax

no trust

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port QoS trust.

Example

no trust

Syntax

bandwidth-ingress <UINT32>

Mode

Switch Controller Port Switch

Description

Configure Ingress Bandwidth.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

bandwidth-ingress 16

Syntax

no bandwidth-ingress

Mode

Switch Controller Port Switch

Description

Disable Ingress Bandwidth.

Example

```
no bandwidth-ingress
```

Syntax

```
bandwidth-egress <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Egress Bandwidth.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
bandwidth-egress 16
```

Syntax

```
no bandwidth-egress
```

Mode

Switch Controller Port Switch

Description

Disable Egress Bandwidth.

Example

```
no bandwidth-egress
```

Syntax

```
security-count <UINT8>
```

Mode

Switch Controller Port Switch

Description

Configure Port Security Max Count.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
security-count 16
```

Syntax

```
no security-count
```

Mode

Switch Controller Port Switch

Description

Disable Port Security Max Count.

Example

```
no security-count
```

Syntax

```
storm-control broadcast <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Storm Control Broadcast Rate.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
storm-control broadcast 16
```

Syntax

```
no storm-control broadcast
```

Mode

Switch Controller Port Switch

Description

Disable Storm Control Broadcast Rate.

Example

```
no storm-control broadcast
```

Syntax

```
storm-control unknown-multicast <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Storm Control Unknown Multicast Rate.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
storm-control unknown-multicast 16
```

Syntax

```
no storm-control unknown-multicast
```

Mode

Switch Controller Port Switch

Description

Disable Storm Control Unknown Multicast Rate.

Example

```
no storm-control unknown-multicast
```

Syntax

```
storm-control unknown-unicast <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Storm Control Unknown Unicast Rate.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
storm-control unknown-unicast 16
```

Syntax

```
no storm-control unknown-unicast
```

Mode

Switch Controller Port Switch

Description

Disable Storm Control Unknown Unicast Rate.

Example

```
no storm-control unknown-unicast
```

Syntax

```
port-8021x config { auto | force-authorized | force-unauthorized }
```

Mode

Switch Controller Port Switch

Description

Configure Switch Controller Port 802.1x Mode.

Options

<i>auto</i>	802.1x Auto Mode
<i>force-authorized</i>	802.1x Force Authorized Mode
<i>force-unauthorized</i>	802.1x Force Unauthorized Mode

Example

```
port-8021x config auto
```

Syntax

```
port-8021x reauth
```

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port 802.1x reauthentication.

Example

```
port-8021x reauth
```

Syntax

```
no port-8021x reauth
```

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port 802.1x reauthentication.

Example

```
no port-8021x reauth
```

Syntax

```
port-8021x reauth-period <UINT16>
```

Mode

Switch Controller Port Switch

Description

Configure Switch Controller Port 802.1x reauth period.

Options

<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: 123

Example

```
port-8021x reauth-period 3600
```

Syntax

port-8021x guest-vlan

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port 802.1x Guest VLAN Assignment.

Example

port-8021x guest-vlan

Syntax

no port-8021x guest-vlan

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port 802.1x Guest VLAN Assignment.

Example

no port-8021x guest-vlan

Syntax

port-8021x radius-vlan-assignment

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port PNAC RADIUS VLAN Assignment.

Example

port-8021x radius-vlan-assignment

Syntax

no port-8021x radius-vlan-assignment

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port 802.1x RADIUS VLAN Assignment.

Example

no port-8021x radius-vlan-assignment

Syntax

```
portshield <CONFIGURABLE_INTERFACE>
```

Mode

Switch Controller Port Switch

Description

Portshield Switch Port to Interface.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
portshield X0
```

Syntax

```
no portshield
```

Mode

Switch Controller Port Switch

Description

Clear Portshield assignment.

Example

```
no portshield
```

Syntax

```
native-vlan <UINT32>
```

Mode

Switch Controller Port Switch

Description

Configure Native Vlan.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
native-vlan 16
```

Syntax

```
no native-vlan
```

Mode

Switch Controller Port Switch

Description

Disable Native Vlan.

Example

```
no native-vlan
```

Syntax

```
vlan-trunk
```

Mode

Switch Controller Port Switch

Description

Enable Switch Controller Port VLAN trunk mode.

Example

```
vlan-trunk
```

Syntax

```
no vlan-trunk
```

Mode

Switch Controller Port Switch

Description

Disable Switch Controller Port VLAN trunk mode.

Example

```
no vlan-trunk
```

Syntax

```
vlan-list <WORD>
```

Mode

Switch Controller Port Switch

Description

Configure Port VLAN list for portshield interface.

Options

<**WORD**> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
vlan-list 201,202
```

Syntax

```
no vlan-list
```

Mode

Switch Controller Port Switch

Description

Removes entry from VLAN list for portshield interface.

Example

```
no vlan-list
```

Syntax

```
switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Add/Edit external switch and enter configuration mode.

Options

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\"

Example

```
switch "My Switch"
```

Syntax

```
name <SWITCH_NAME>
```

Mode

Switch

Description

Set external switch name.

Options

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\"

Example

```
name LAN_SWS12-48
```

Syntax

```
authorize <SWITCH_PENDING_NAME>
```

Mode

Switch Controller

Description

Authorize SonicWall to add a switch and configure with default configuration.

Options

<SWITCH_PENDING_NAME> Switch Name in Pending List.
Example: \ "My Switch\"

Example

```
authorize "My Switch"
```

Syntax

restart <SWITCH_NAME>

Mode

Switch Controller

Description

Restart a SonicWall Switch.

Options

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\"

Example

restart "My Switch"

Syntax

upgrade <SWITCH_NAME> *partition* <UINT32> *version* <WORD>

Mode

Switch Controller

Description

Upgrade firmware.

Options

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\"

partition Boot partition.

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

version Firmware version.

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

upgrade CoreSwitch *partition* 1 *version* 1.0.0.0-35

Syntax

model { *sws12-10fpoe* | *sws12-8* | *sws12-8poe* | *sws14-24* | *sws14-24fpoe* | *sws14-48* | *sws14-48fpoe* }

Mode

Switch

Description

External switch model.

Options

sws12-10fpoe SonicWall Switch SWS12-10FPOE

sws12-8 SonicWall Switch SWS12-8

sws12-8poe SonicWall Switch SWS12-8POE

<i>sws14-24</i>	SonicWall Switch SWS14-24
<i>sws14-24fpo</i>	SonicWall Switch SWS14-24FPOE
<i>sws14-48</i>	SonicWall Switch SWS14-48
<i>sws14-48fpo</i>	SonicWall Switch SWS14-48FPOE

Example

```
model sws12-10fpo
```

Syntax

```
no switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Delete external switch.

Options

```
<SWITCH_NAME> Switch Name.  
Example: \ "My Switch\ "
```

Example

```
no switch "My Switch"
```

Syntax

```
serial <WORD>
```

Mode

Switch

Description

Set external switch serial number.

Options

```
<WORD> Word in the form: WORD or \"QUOTED STRING\".  
Example: abc
```

Example

```
serial 2CB8ED4B1210
```

Syntax

```
comment <WORD>
```

Mode

Switch

Description

Set external switch description.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment LAN_Switch
```

Syntax

```
ip <IPV4_HOST>
```

Mode

Switch

Description

Set IPv4 Address of the Switch configured in the Extended Switch Instance.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
ip 10.10.10.200
```

Syntax

```
user-name <WORD>
```

Mode

Switch

Description

Set Extended Switch Username.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
user-name admin
```

Syntax

```
password <ENC_PASSWORD>
```

Mode

Switch

Description

Set Extended Switch Password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
password pwd1234
```

Syntax

active-partition <UINT32>

Mode

Switch

Description

Set external switch Active Partition.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

active-partition 1

Syntax

switch-mode { *daisy-chain* | *standalone* }

Mode

Switch

Description

Select Extended Switch Mode - Standalone or DaisyChain.

Options

daisy-chain Daisy chain mode.

standalone Standalone mode.

Example

switch-mode standalone

Syntax

uplink <INT32>

Mode

Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<INT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

uplink 1

Syntax

```
firewall-uplink <CONFIGURABLE_INTERFACE>
```

Mode

Switch

Description

Set Firewall Interface connected to the Extended Switch.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
firewall-uplink X0
```

Syntax

```
no firewall-uplink
```

Mode

Switch

Description

Clear Firewall Interface connected to the Extended Switch.

Example

```
no firewall-uplink
```

Syntax

```
management <UINT32>
```

Mode

Switch

Description

Set Extended Switch Management Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
management 1
```

Syntax

```
uplink-secondary <INT32>
```

Mode

Switch

Description

Set Extended Switch Interface connected to the Standalone/Secondary Firewall.

Options

<INT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

uplink-secondary 1

Syntax

management-secondary <UINT32>

Mode

Switch

Description

Set Extended Switch Management Interface connected to the Standalone/Secondary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

management-secondary 1

Syntax

parent-switch-name <SWITCH_NAME>

Mode

Switch

Description

Name of the Parent Switch.

Options

<SWITCH_NAME> Switch Name.
Example: *\ "My Switch\"*

Example

parent-switch-name LAN_SWS12-48

Syntax

parent-switch-uplink <UINT32>

Mode

Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

parent-switch-uplink 1

Syntax

no parent-switch-uplink

Mode

Switch

Description

Clear Extended Switch Interface connected to the Standalone/Primary Firewall.

Example

no parent-switch-uplink

Syntax

stp-mode { multiple | rapid }

Mode

Switch

Description

Select STP Operation Mode configured on the Extended Switch.

Options

multiple Multiple mode.

rapid Rapid mode.

Example

stp-mode rapid

Syntax

stp

Mode

Switch

Description

Enable Global STP State configured on SonicWall Switch.

Example

stp

Syntax

no stp

Mode

Switch

Description

Disable Global STP State configured on SonicWall Switch.

Example

```
no stp
```

Syntax

```
switch-8021x
```

Mode

Switch

Description

Enable Global 802.1x State configured on the Extended Switch.

Example

```
switch-8021x
```

Syntax

```
no switch-8021x
```

Mode

Switch

Description

Disable Global 802.1x State configured on the Extended Switch.

Example

```
no switch-8021x
```

Syntax

```
switch-8021x-guest-vlan
```

Mode

Switch

Description

Enable Global 802.1x Guest VLAN State configured on the Extended Switch.

Example

```
switch-8021x-guest-vlan
```

Syntax

```
no switch-8021x-guest-vlan
```

Mode

Switch

Description

Disable Global 802.1x Guest VLAN State configured on the Extended Switch.

Example

```
no switch-8021x-guest-vlan
```

Syntax

```
switch-8021x-guest-vlan-id <UINT32>
```

Mode

Switch

Description

Set Global 802.1x Guest VLAN ID for Extended Switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
switch-8021x-guest-vlan-id 200
```

Syntax

```
jumbo-frame-size <UINT32>
```

Mode

Switch

Description

Set Global PNAC Guest VLAN ID for Extended Switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
jumbo-frame-size 9000
```

Syntax

```
voice-vlan <SWITCH_NAME>
```

Mode

Switch Controller

Description

Voice Vlan Configuration.

Options

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\ "

Example

```
voice-vlan switch abcd
```

Syntax

```
state { auto | disabled }
```

Mode

Switch Controller Voice Vlan

Description

Voice Vlan state Configuration.

Options

auto Auto Voice Vlan.

disabled Disable Voice Vlan.

Example

```
state auto
```

Syntax

```
vlan <UINT32>
```

Mode

Switch Controller Voice Vlan

Description

Voice Vlan state Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
vlan 1
```

Syntax

```
priority-tag <UINT32>
```

Mode

Switch Controller Voice Vlan

Description

Voice Vlan Priority Tag Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
priority-tag 1
```

Syntax

```
dscp <UINT32>
```

Mode

Description

Voice Vlan DSCP Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

dscp 1

Syntax

radius <WORD> switch <SWITCH_NAME>

Mode

Switch Controller

Description

Configure Radius Server.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
switch Configure Snwl Switch.
<SWITCH_NAME> Switch Name.
Example: \"My Switch\"

Syntax

no radius <WORD> switch <SWITCH_NAME>

Mode

Switch Controller

Description

Delete Radius Server.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: abc
switch Snwl Switch.
<SWITCH_NAME> Switch Name.
Example: \"My Switch\"

Syntax

authorized-port <UINT32>

Mode

Radius Server

Description

Authorized Port Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

authorized-port 3

Syntax

key-string **<WORD>**

Mode

Radius Server

Description

key String Configuration.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

ey-string abc

Syntax

timeout-reply **<UINT32>**

Mode

Radius Server

Description

Timeou Reply Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

timeout-reply 2

Syntax

retry **<UINT32>**

Mode

Radius Server

Description

Retry Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

retry 2

Syntax

```
user <WORD> switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Selecting switch to add/edit user.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
switch	switch for external switch.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Example

```
user user100 switch myswitch
```

Syntax

```
no user <WORD> switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Selecting switch to user.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
switch	switch for external switch.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Example

```
no user user100 switch myswitch
```

Syntax

```
password <WORD>
```

Mode

User

Description

Set Password for user.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
password pwd1234
```

Syntax

```
privilege-type { admin | user }
```

Mode

User

Description

Select user privilege-type - admin or user.

Options

admin Providing ADMIN privileges to the user.

user Non-admin privileges to the user.

Example

```
privilege-type admin
```

Syntax

```
network <UINT16> switch <SWITCH_NAME>
```

Mode

Switch Controller

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

switch Configure switch name.

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\ "

Example

```
network 3 switch switch1
```

Syntax

```
no network <UINT16> switch <SWITCH_NAME>
```

Mode

Switch Controller

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

switch Delete network by switch name.

<SWITCH_NAME> Switch Name.
Example: \ "My Switch\ "

Example

```
no network 3 switch switch1
```

Syntax


```
ip { dhcp | static <IPV4_HOST> <IPV4_MASK> }
```

Mode

Switch Controller Network

Description

Configure network ip on switch.

Options

<i>dhcp</i>	Ip address assigned by DHCP.
<i>static</i>	Static Ip address assigned.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i><IPV4_MASK></i>	IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: <i>255.255.255.0</i>

Example

```
ip dhcp
ip static <switchNetwAddr> <switchNetwMask>
```

Syntax

```
dns primary <IPV4_HOST>
```

Mode

Switch Controller Network

Description

Configure DNS for switch network.

Options

<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>

Example

```
dns primary 10.5.3.23
```

Syntax

```
no dns primary
```

Mode

Switch Controller Network

Description

Clear DNS for switch network.

Example

```
no dns primary
```

Syntax

```
dns secondary <IPV4_HOST>
```

Mode

Description

Configure DNS for switch network.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

dns secondary 8.8.4.4

Syntax

no dns secondary

Mode

Switch Controller Network

Description

Clear DNS for switch network.

Example

no dns secondary

Syntax

route switch <SWITCH_NAME> destination <IPV4_HOST> netmask <SWITCH_ROUTE_MASK> gateway <IPV4_HOST>

Mode

Switch Controller

Options

switch	Configure switch name
<SWITCH_NAME>	Switch Name. Example: \"My Switch\"
destination	Set destination for static route.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168
netmask	Set netmask for static route.
<SWITCH_ROUTE_MASK>	IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: 255.255.255.0
gateway	Set gateway for static route.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: 192.168.168.168

Example

route switch 2CB8ED4B14F6 destination 192.168.9.0 netmask 255.255.255.0

Syntax

no route switch <SWITCH_NAME> destination <IPV4_HOST> netmask <SWITCH_ROUTE_MASK>

Mode

Switch Controller

Description

Delete static route.

Options

<i>switch</i>	Configure switch name
<i><SWITCH_NAME></i>	Switch Name. Example: <code>\ "My Switch\ "</code>
<i>destination</i>	Set destination for static route.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <code>192.168.168.168</code>
<i>netmask</i>	Set netmask for static route.
<i><SWITCH_ROUTE_MASK></i>	IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: <code>255.255.255.0</code>

Example

```
no route switch switchName destination 192.168.9.0 netmask 255.255.255.0
```

Syntax

```
arp mac <MAC> vlan <UINT16> switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Configure static mac address on switch.

Options

<i>mac</i>	Configure switch mac address.
<i><MAC></i>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <code>00:0C:F1:56:98:AD</code>
<i>vlan</i>	Retrieve Vlan of the mac address.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <code>123</code>
<i>switch</i>	Retrive switch for MAC.
<i><SWITCH_NAME></i>	Switch Name. Example: <code>\ "My Switch\ "</code>

Example

```
arp mac 88:12:21:a0:0f:54 vlan 2 switch switch1
```

Syntax

```
no arp mac <MAC> vlan <UINT16> switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Delete static mac address on switch.

Options

<i>mac</i>	Configure switch mac address.
<i><MAC></i>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <code>00:0C:F1:56:98:AD</code>
<i>vlan</i>	Retrieve Vlan of the mac address.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <code>123</code>
<i>switch</i>	Retrive switch for MAC.
<i><SWITCH_NAME></i>	Switch Name. Example: <code>\ "My Switch\ "</code>

Example

```
no arp mac 88:12:21:a0:0f:54 vlan 2 switch switch1
```

Syntax

```
port <UINT16>
```

Mode

Switch Controller Network

Description

Configure port number for mac address.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
port 3
```

Syntax

```
arp-aging-time switch <SWITCH_NAME>
```

Mode

Switch Controller

Options

switch Retrive switch for MAC agingtime.
<SWITCH_NAME> Switch Name.
Example: \ "My Switch\ "

Example

```
arp-aging-time switch switch1
```

Syntax

```
aging-time <UINT16>
```

Mode

Switch Controller Network

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
aging-time 300
```

Syntax

```
qos switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

Configure qos for switch.

Options

- switch* Retrive switch for QoS.
- <SWITCH_NAME>* Switch Name.
Example: `\ "My Switch\"`

Example

`qos switch switch1`

Syntax

`enable`

Mode

Switch Controller QoS

Description

Enable qos for switch.

Example

`enable`

Syntax

`no enable`

Mode

Switch Controller QoS

Description

Disable qos for switch.

Example

`no enable`

Syntax

`schedule-method { strict-priority | weighted-round-robin }`

Mode

Switch Controller QoS

Description

Scheduling method for switch QoS.

Options

- strict-priority* Strict priority queue.
- weighted-round-robin* Strict priority queue.

Example

`schedule-method strict-priority`

Syntax

```
trust-mode { 8021p | dscp | dscp-8021p }
```

Mode

Switch Controller QoS

Description

Trust mode for switch QoS.

Options

8021p	802.1p.
dscp	DSCP.
dscp-8021p	802.1p-DSCP.

Example

```
trust-mode dscp-8021p
```

Syntax

```
round-robin-weight1 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 1.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
round-robin-weight1 10
```

Syntax

```
no round-robin-weight1
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight1
```

Syntax

```
round-robin-weight2 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 2.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight2 10
```

Syntax

```
no round-robin-weight2
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight2
```

Syntax

```
round-robin-weight3 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 3.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight3 10
```

Syntax

```
no round-robin-weight3
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight3
```

Syntax

```
round-robin-weight4 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 4.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight4 10
```

Syntax

```
no round-robin-weight4
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight4
```

Syntax

```
round-robin-weight5 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 5.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight5 10
```

Syntax

```
no round-robin-weight5
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight5
```

Syntax

```
round-robin-weight6 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 6.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight6 10
```

Syntax

```
no round-robin-weight6
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight6
```

Syntax

```
round-robin-weight7 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 7.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
round-robin-weight7 10
```

Syntax

```
no round-robin-weight7
```

Mode

Switch Controller QoS

Example

```
no round-robin-weight7
```

Syntax

```
round-robin-weight8 <UINT16>
```

Mode

Switch Controller QoS

Description

Weight for Queue 8.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

round-robin-weight8 10

Syntax

no round-robin-weight8

Mode

Switch Controller QoS

Example

no round-robin-weight8

Syntax

qos-dscp switch <SWITCH_NAME>

Mode

Switch Controller

Description

DSCP configuration for switch.

Options

switch Retrive switch for QoS.
<SWITCH_NAME> Switch Name.
Example: *\ "My Switch\ "*

Example

qos-dscp switch switch1

Syntax

dscp-id <UINT8> queue-id <UINT8>

Mode

Switch Controller QoS DSCP

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*
queue-id Configure switch QoS dscp queue.
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

dscp-id 30 queue-id 2

Syntax

```
qos-cos switch <SWITCH_NAME>
```

Mode

Switch Controller

Description

CoS configuration for switch.

Options

- switch** Retrive switch for QoS.
- <SWITCH_NAME>** Switch Name.
Example: `\ "My Switch\ "`

Example

```
qos-cos switch switch1
```

Syntax

```
cos-id <UINT8> queue-id <UINT8>
```

Mode

Switch Controller QoS CoS

Options

- <UINT8>** Integer in the form: D OR 0xHH.
Example: `123`
- queue-id** Configure switch QoS CoS queue.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: `123`

Example

```
cos-id 30 queue-id 2
```

Syntax

```
show switch-controller switch [ <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show Switch Configuration.

Options

- <SWITCH_NAME>** Switch Name.
Example: `\ "My Switch\ "`

Example

```
show switch-controller switch "LAN Switch"
```

Syntax

```
show switch-controller voice-vlan [ <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show Voice Vlan configuration or Status.

Options

<SWITCH_NAME> Switch Name.
Example: `\ "My Switch\"`

Example

```
show switch-controller voice-vlan switch "LAN Switch"
```

Syntax

```
show switch-controller user [ <WORD> switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show users configuration or status.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

switch Show users configuration by switch name.

<SWITCH_NAME> Switch Name.
Example: `\ "My Switch\"`

Example

```
show switch-controller user user100 switch "LAN Switch"
```

Syntax

```
show switch-controller port [ <WORD> switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show port configuration or Status.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`

switch Show port configuration by switch name.

<SWITCH_NAME> Switch Name.
Example: `\ "My Switch\"`

Example

```
show switch-controller port 2 switch LANSwitch
```

Syntax

```
show switch-controller network [ <UINT16> switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch controller network.

Options

<UINT16>	Integer in the form: D OR 0xHHHH. Example: 123
switch	Switch of network.
<SWITCH_NAME>	Switch Name. Example: \ "My Switch\ "

Syntax

```
show switch-controller radius [ <IPV4_HOST> switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show radius server configuration or status.

Options

<IPV4_HOST>	IPV4 Address in the form: a.b.c.d. Example: 192.168.168.168
switch	Show radius server configuration by switch name.
<SWITCH_NAME>	Switch Name. Example: \ "My Switch\ "

Example

```
show switch-controller radius 1.1.1.1 switch "LAN Switch"
```

Syntax

```
show switch-controller route
```

Mode

All Modes

Description

show static route configuration or Status.

Example

```
show switch-controller route switch "abcd"
```

Syntax

```
show switch-controller arp [ mac <MAC> vlan <UINT16> switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch controller arp.

Options

mac	Mac Address.

<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
vlan	VLAN of the switch.
<UINT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
switch	Switch of network.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Syntax

```
show switch-controller arp-aging-time [ switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch mac address aging time.

Options

switch	Switch of MAC.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Syntax

```
show switch-controller qos [ switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch QoS Config.

Options

switch	Switch for QoS.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Syntax

```
show switch-controller qos-dscp [ switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch QoS DSCP Config.

Options

switch	Switch for QoS.
<SWITCH_NAME>	Switch Name. Example: <i>\ "My Switch\"</i>

Syntax

```
show switch-controller qos-cos [ switch <SWITCH_NAME> ]
```

Mode

All Modes

Description

Show switch QoS CoS Config.

Options

- switch** Switch for QoS.
- <SWITCH_NAME>** Switch Name.
Example: `\ "My Switch\"`

Syntax

```
dell-switch
```

Mode

Config

Description

Enter Dell Switch mode.

Example

```
dell-switch
```

Syntax

```
port <WORD> switch <UINT32>
```

Mode

Dell Switch

Description

Dell Switch Port Mode.

Options

- <WORD>** Word in the form: WORD or \"QUOTED STRING\".
Example: `abc`
- switch** Switch.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHH.
Example: `123`

Example

```
port 5 switch 1
```

Syntax

```
clear-statistics switch <UINT32>
```

Mode

Dell Switch

Description

Clear Switch Statistics.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

clear-statistics switch 1

Syntax

enable

Mode

Dell Switch Port Switch

Description

Enable Dell Switch Port.

Example

enable

Syntax

no enable

Mode

Dell Switch Port Switch

Description

Disable Dell Switch Port.

Example

no enable

Syntax

link-speed { auto-negotiate | full { { 10 | 100 | 1000 | 10000 } } | half { { 10 | 100 } } }

Mode

Dell Switch Port Switch

Description

Configure port link speed.

Options

<i>auto-negotiate</i>	Set port link speed to auto-negotiate
<i>full</i>	Full duplex.
<i>10</i>	10 Mbps - Full Duplex
<i>100</i>	100 Mbps - Full Duplex
<i>1000</i>	1000 Mbps - Full Duplex
<i>10000</i>	10000 Mbps - Full Duplex
<i>half</i>	Half duplex.

10	10 Mbps - Half Duplex
100	100 Mbps - Half Duplex

Example

link-speed auto-negotiate

Syntax

stp

Mode

Dell Switch Port Switch

Description

Enable STP for Port.

Example

stp

Syntax

no stp

Mode

Dell Switch Port Switch

Description

Disable STP for Port.

Example

no stp

Syntax

poe

Mode

Dell Switch Port Switch

Description

Dell Switch Port POE Status.

Example

poe

Syntax

no poe

Mode

Dell Switch Port Switch

Description

Dell Switch Port POE Status.

Example

```
no poe
```

Syntax

```
portshield-uplink
```

Mode

Dell Switch Port Switch

Description

Enable dedicated uplink for port's portshield interface.

Example

```
portshield-uplink
```

Syntax

```
no portshield-uplink
```

Mode

Dell Switch Port Switch

Description

Disable dedicated uplink for port's portshield interface.

Example

```
no portshield-uplink
```

Syntax

```
portshield-uplink-secondary
```

Mode

Dell Switch Port Switch

Description

Enable secondary dedicated uplink for port's portshield interface.

Example

```
portshield-uplink-secondary
```

Syntax

```
no portshield-uplink-secondary
```

Mode

Dell Switch Port Switch

Description

Disable secondary dedicated uplink for port's portshield interface.

Example

Syntax

```
poe-priority { critical | high | low }
```

Mode

Dell Switch Port Switch

Description

Configure port POE power priority level.

Options

critical Critical

high High

low low

Example

```
poe-priority critical
```

Syntax

```
power-limit <UINT16>
```

Mode

Dell Switch Port Switch

Description

Configure port POE power limit.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
power-limit 10
```

Syntax

```
no power-limit
```

Mode

Dell Switch Port Switch

Description

Diable port POE power limit.

Example

```
no power-limit
```

Syntax

```
portshield <CONFIGURABLE_INTERFACE>
```

Mode

Dell Switch Port Switch

Description

Portshield Switch Port to Interface.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
portshield X0
```

Syntax

```
no portshield
```

Mode

Dell Switch Port Switch

Description

Clear Portshield assignment.

Example

```
no portshield
```

Syntax

```
vlan-trunk
```

Mode

Dell Switch Port Switch

Description

Enable Dell Switch Port VLAN trunk mode.

Example

```
vlan-trunk
```

Syntax

```
no vlan-trunk
```

Mode

Dell Switch Port Switch

Description

Disable Dell Switch Port VLAN trunk mode.

Example

```
no vlan-trunk
```

Syntax

```
vlan-list <WORD>
```

Mode

Dell Switch Port Switch

Description

Configure Port VLAN list for portshield interface.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
vlan-list 201,202
```

Syntax

```
no vlan-list
```

Mode

Dell Switch Port Switch

Description

Removes entry from VLAN list for portshield interface.

Example

```
no vlan-list
```

Syntax

```
switch <UINT32>
```

Mode

Dell Switch

Description

Add/Edit external switch and enter configuration mode.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
switch "My Switch"
```

Syntax

```
switch-restart <UINT32>
```

Mode

Dell Switch

Description

Restart a Dell Switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

switch-restart 1

Syntax

model { n1108p-on | n1108t-on | n1124p-on | n1124t-on | n1148p-on | n1148t-on | n1524 | n1524p | n1548 | n1548p | n2024 | n2024p | n2048 | n2048p | n2128px-on | n3024 | n3024f | n3024p | n3048 | n3048p | n3132px-on | x1008 | x1008p | x1018 | x1018p | x1026 | x1026p | x1052 | x1052p | x4012 }

Mode

Switch

Description

External switch model.

Options

- n1108p-on Dell Switch N1108P-ON
- n1108t-on Dell Switch N1108T-ON
- n1124p-on Dell Switch N1124P-ON
- n1124t-on Dell Switch N1124T-ON
- n1148p-on Dell Switch N1148P-ON
- n1148t-on Dell Switch N1148T-ON
- n1524 Dell Switch N1524
- n1524p Dell Switch N1524P
- n1548 Dell Switch N1548
- n1548p Dell Switch N1548P
- n2024 Dell Switch N2024
- n2024p Dell Switch N2024P
- n2048 Dell Switch N2048
- n2048p Dell Switch N2048P
- n2128px-on Dell Switch N2128PX-ON
- n3024 Dell Switch N3024
- n3024f Dell Switch N3024F
- n3024p Dell Switch N3024P
- n3048 Dell Switch N3048
- n3048p Dell Switch N3048P
- n3132px-on Dell Switch N3132PX-ON

<i>x1008</i>	Dell Switch X1008
<i>x1008p</i>	Dell Switch X1008
<i>x1018</i>	Dell Switch X1018
<i>x1018p</i>	Dell Switch X1018P
<i>x1026</i>	Dell Switch X1026
<i>x1026p</i>	Dell Switch X1008
<i>x1052</i>	Dell Switch X1052
<i>x1052p</i>	Dell Switch X1052P
<i>x4012</i>	Dell Switch X4012

Example

```
model x1026
```

Syntax

```
no switch <UINT32>
```

Mode

Dell Switch

Description

Delete external switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
no switch 1
```

Syntax

```
serial <WORD>
```

Mode

Switch

Description

Set external switch serial number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
serial 2CB8ED4B1210
```

Syntax

comment <WORD>

Mode

Switch

Description

Set external switch description.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

comment LAN_Switch

Syntax

ip <IPV4_HOST>

Mode

Switch

Description

Set IPv4 Address of the Switch configured in the Extended Switch Instance.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

ip 10.10.10.200

Syntax

user-name <WORD>

Mode

Switch

Description

Set Extended Switch Username.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name admin

Syntax

password <WORD>

Mode

Switch

Description

Set Extended Switch Password.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

password pwd1234

Syntax

switch-mode { daisy-chain | standalone }

Mode

Switch

Description

Select Extended Switch Mode - Standalone or DaisyChain.

Options

daisy-chain Daisy chain mode.

standalone Standalone mode.

Example

switch-mode standalone

Syntax

uplink <INT32>

Mode

Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<INT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

uplink 1

Syntax

firewall-uplink <CONFIGURABLE_INTERFACE>

Mode

Switch

Description

Set Firewall Interface connected to the Extended Switch.

Options

<CONFIGURABLE_INTERFACE> Interface name.
Example: *X0*

Example

```
firewall-uplink X0
```

Syntax

```
no firewall-uplink
```

Mode

Switch

Description

Clear Firewall Interface connected to the Extended Switch.

Example

```
no firewall-uplink
```

Syntax

```
management <UINT32>
```

Mode

Switch

Description

Set Extended Switch Management Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
management 1
```

Syntax

```
parent-switch-id <UINT32>
```

Mode

Switch

Description

Name of the Parent Switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
parent-switch-id 2
```

Syntax

parent-switch-uplink <UINT32>

Mode

Switch

Description

Set Extended Switch Interface connected to the Standalone/Primary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

parent-switch-uplink 1

Syntax

no parent-switch-uplink

Mode

Switch

Description

Clear Extended Switch Interface connected to the Standalone/Primary Firewall.

Example

no parent-switch-uplink

Syntax

uplink-secondary <INT32>

Mode

Switch

Description

Set Extended Switch Interface connected to the Secondary Firewall.

Options

<INT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

uplink-secondary 1

Syntax

management-secondary <UINT32>

Mode

Switch

Description

Set Extended Switch Management Interface connected to the Secondary Firewall.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

management-secondary 1

Syntax

stp-mode { classic | multiple | rapid }

Mode

Switch

Description

Select STP Operation Mode configured on the Extended Switch.

Options

classic Classic mode.

multiple Multiple mode.

rapid Rapid mode.

Example

stp-mode rapid

Syntax

stp

Mode

Switch

Description

Enable Global STP State configured on the Extended Switch.

Example

stp

Syntax

no stp

Mode

Switch

Description

Disable Global STP State configured on the Extended Switch.

Example

no stp

Syntax

```
poe-threshold <UINT32>
```

Mode

Switch

Description

Set POE Usage threshold value for dell switch.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
poe-threshold 95
```

Syntax

```
poe-traps
```

Mode

Switch

Description

Enable POE Traps for X-series dell switch.

Example

```
poe-traps
```

Syntax

```
no poe-traps
```

Mode

Switch

Description

Disable POE Traps for X-series dell switch.

Example

```
no poe-traps
```

Syntax

```
power-limit-type { poe-class-limit | poe-port-limit }
```

Mode

Switch

Description

Set Power Limit Type for x-series dell switch.

Options

poe-class-limit POE Power Limit Class Limit.

poe-port-limit POE Power Limit Port Limit.

Example

```
power-limit-type poe-port-limit
```

Syntax

```
poe-management-mode { class | dynamic | static }
```

Mode

Switch

Description

Set POE Management mode for N-series dell switch.

Options

class Class management mode.

dynamic Dynamic management mode.

static Static management mode.

Example

```
poe-management-mode dynamic
```

Syntax

```
poe-detection-type { dot-legacy | legacy }
```

Mode

Switch

Description

Set POE Detection Type for N-series dell switch.

Options

dot-legacy POE Detection type Dot Legacy.

legacy POE Detection Type Legacy.

Example

```
poe-detection-type dot-legacy
```

Syntax

```
show dell-switch switch [ <UINT32> ]
```

Mode

All Modes

Description

Show Switch Configuration.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

show dell-switch switch 1

Syntax

show dell-switch port [<WORD> switch <UINT32>]

Mode

All Modes

Description

Show port configuration or Status.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

switch Show port configuration by switch ID.

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

show dell-switch port 2 switch 1

Syntax

show dell-switch statistics switch <UINT32>

Mode

All Modes

Description

Show dell-switch statistics information.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

show dell-switch statistics switch 1

Syntax

show dell-switch firmware-mgmt switch <UINT32>

Mode

All Modes

Description

Show dell-switch firmware management information.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.

Example: 123

Example

```
show dell-switch firmware-mgmt switch 1
```

Syntax

```
show dell-switch ports
```

Mode

All Modes

Description

Show dell-switch ports information.

Example

```
show dell-switch ports
```

Syntax

```
show dell-switch status
```

Mode

All Modes

Description

Show dell-switch status information.

Example

```
show dell-switch status
```

Syntax

```
show dell-switch product-info
```

Mode

All Modes

Description

Show dell-switch Product information.

Example

```
show dell-switch product-info
```

Syntax

```
wireless
```

Mode

Config

Description

Enter wireless configuration mode.

Example

wireless

Syntax

radio-role { access-point | access-point-station | wds-station }

Mode

Wireless

Description

Select radio role and enter configuration mode.

Options

- access-point*** Configure as access point.
- access-point-station*** Configure as access point & station mode.
- wds-station*** Configure as wireless wds station.

Example

radio-role access-point
radio-role wds-station

Syntax

enable

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Enable WLAN wireless.

Example

enable

Syntax

no enable

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Disable WLAN wireless.

Example

no enable

Syntax

```
ssid <WORD>
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set the wireless SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ssid sonicwall
```

Syntax

```
short-guard-interval
```

Mode

Access Point
Wireless Bridge

Description

Enable short guard interval.

Example

```
short-guard-interval
```

Syntax

```
no short-guard-interval
```

Mode

Access Point
Wireless Bridge

Description

Disable short guard interval.

Example

```
no short-guard-interval
```

Syntax

```
aggregation
```

Mode

Access Point
Wireless Bridge

Description

Enable aggregation.

Example

aggregation

Syntax

no aggregation

Mode

Access Point
Wireless Bridge

Description

Disable aggregation.

Example

no aggregation

Syntax

threshold fragmentation <UINT16>

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set wireless fragmentation threshold in bytes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

threshold fragmentation 2346

Syntax

threshold rts <UINT16>

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set wireless RTS threshold in bytes.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

threshold rts 2346

Syntax

```
authentication-type { wep { { both | open-system | shared-key } } | wpa { { eap | psk } } | wpa2 { { auto { { eap | psk } } | eap | psk } } | wpa3 { { eap | eap-192b | owe | psk | wpa2-auto { { eap | psk } } } } }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set wep/wpa authentication type.

Options

wep	WEP.
both	WEP - both (open system and shared key).
open-system	WEP - open system.
shared-key	WEP - shared key.
wpa	WPA.
eap	WPA - EAP.
psk	WPA - PSK.
wpa2	WPA2.
auto	WPA2 - AUTO.
eap	Wpa2 - AUTO - EAP.
psk	Wpa2 - AUTO - PSK.
eap	Wpa2 - EAP.
psk	Wpa2 - PSK.
wpa3	WPA3.
eap	WPA3 - EAP.
eap-192b	WPA3 - EAP - 192B.
owe	WPA3 - OWE.
psk	WPA3 - PSK.
wpa2-auto	WPA3/WPA2 - AUTO.
eap	WPA3/WPA2 - EAP.
psk	WPA3/WPA2 - PSK.

Example

```
authentication-type wep both
```

Syntax

```
wep-key { { key1 | key2 | key3 | key4 } { { type { 128 | 152 | 64 } value <ENC_PASSWORD> } } | default { { 1 | 2 | 3 | 4 } } | method { { alphanumeric | hexadecimal } } }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set WEP key configuration.

Options

<i>key1</i>	Set WEP key1 type and value.
<i>key2</i>	Set WEP key2 type and value.
<i>key3</i>	Set WEP key3 type and value.
<i>key4</i>	Set WEP key4 type and value.
<i>type</i>	Set WEP key type.
<i>128</i>	128 bits.
<i>152</i>	152 bits.
<i>64</i>	64 bits.
<i>value</i>	Set WEP key value.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>
<i>default</i>	Set WEP default key.
<i>1</i>	WEP default key1.
<i>2</i>	WEP default key2.
<i>3</i>	WEP default key3.
<i>4</i>	WEP default key3.
<i>method</i>	Set WEP key method.
<i>alphanumeric</i>	Alphanumeric.
<i>hexadecimal</i>	Hexadecimal.

Example

```
wep-key method alphanumeric
wep-key default 2
wep-key 2 type 64 value wepVa
```

Syntax

```
no wep-key { key1 | key2 | key3 | key4 }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Clear wireless WEP key setting.

Options

key1 Clear WEP key1 type and value.

key2 Clear WEP key2 type and value.

key3 Clear WEP key3 type and value.

key4 Clear WEP key4 type and value.

Example

```
no wep-key 2 type
no wep-key 2 value
```

Syntax

```
eapol-version { v1 | v2 }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set WPA EAPOL version.

Options

v1 EAPOL version1.

v2 EAPOL version2.

Example

```
eapol-version v2
```

Syntax

```
wpa cipher-type { aes | auto | gcmp | tkip }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set WPA cipher type.

Options

aes AES.

auto Auto.

gcmp AES-GCMP.

tkip TKIP.

Example

```
wpa cipher-type aes
```

Syntax

```
wpa passphrase <ENC_PASSWORD>
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
wpa passphrase password
```

Syntax

```
no wpa passphrase
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Clear WPA passphrase.

Example

```
no wpa passphrase
```

Syntax

```
connect <DETECTED_ACCESS_POINT_SSID>
```

Mode

Wireless Bridge
Wireless AccessPoint&Station

Description

Connect to the specified access point.

Options

<DETECTED_ACCESS_POINT_SSID> Detected access point SSID.
Example: *sonicwall*

Example

```
connect sonicwall
```

Syntax

```
scan
```

Mode

Wireless Bridge
Wireless AccessPoint&Station

Description

Scan nearby access points.

Example

```
scan
```

Syntax

```
wireless-interface-as-wan
```

Mode

Wireless Bridge

Description

Enable wireless interface as WAN.

Example

```
wireless-interface-as-wan
```

Syntax

```
no wireless-interface-as-wan
```

Mode

Wireless Bridge

Description

Disable wireless interface as WAN.

Example

```
no wireless-interface-as-wan
```

Syntax

```
connectivity-check
```

Mode

Wireless Bridge

Description

Enable wireless client connectivity check and auto reconnect.

Example

```
connectivity-check
```

Syntax

```
no connectivity-check
```

Mode

Wireless Bridge

Description

Disable wireless client connectivity check and auto reconnect.

Example

```
no connectivity-check
```

Syntax

```
remote-ip <IPV4_HOST>
```

Mode

Wireless Bridge

Description

Set target remote IP(make sure the specified IP is pingable) to ping.

Options

<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

Example

```
remote-ip 192.168.168.168
```

Syntax

```
no remote-ip
```

Mode

Wireless Bridge

Description

Clear target remote IP to ping.

Example

```
no remote-ip
```

Syntax

```
antenna-diversity best
```

Mode

Wireless Bridge

Description

Set wireless antenna diversity.

Options

best Best.

Example

```
antenna-diversity best
```

Syntax

```
restore-default
```

Mode

Wireless Bridge

Description

Restore advanced wireless settings to default.

Example

```
restore-default
```

Syntax

```
block-station <DETECTED_WIRELESS_STATION_MAC>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Block specified station.

Options

<DETECTED_WIRELESS_STATION_MAC> Detected wireless station MAC address.
Example: *00:0C:F1:56:98:AD*

Example

```
block 00:19:D2:05:72:F4
```

Syntax

```
allow-station <DETECTED_WIRELESS_STATION_MAC>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Allow specified station.

Options

<DETECTED_WIRELESS_STATION_MAC> Detected wireless station MAC address.
Example: *00:0C:F1:56:98:AD*

Example

```
allow-station 00:19:D2:05:72:F4
```

Syntax

```
disassociate-station <DETECTED_WIRELESS_STATION_MAC>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Logout and disassociate specified station.

Options

<DETECTED_WIRELESS_STATION_MAC> Detected wireless station MAC address.
Example: *00:0C:F1:56:98:AD*

Example

disassociate-station 00:19:D2:05:72:F4

Syntax

disassociate-stations

Mode

Access Point
Wireless AccessPoint&Station

Description

Logout and disassociate all stations.

Example

disassociate-stations

Syntax

schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }

Mode

Access Point
Wireless AccessPoint&Station

Description

Set the schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i><SCHED_TIME_END></i>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "Work Hours"

Syntax

country-code <WIRELESS_COUNTRY_CODE>

Mode

Description

Set wireless country code.

Options

<WIRELESS_COUNTRY_CODE> Wireless country code.
Example: *United States*

Example

country-code "United States"

Syntax

radio mode { 5000mhz { { a-only | ac-na-mixed | ac-only | n-only | na-mixed } } | g-only | gb-mixed | n-only | ngb-mixed }

Mode

Description

Set the wireless mode.

Options

- 5000mhz** 5GHz.
- a-only** 5GHz 802.11a only.
- ac-na-mixed** 5GHz 802.11ac/n/a mixed.
- ac-only** 5GHz 802.11ac only.
- n-only** 5GHz 802.11n only.
- na-mixed** 5GHz 802.11n/a mixed.
- g-only** 2.4GHz 802.11g only.
- gb-mixed** 2.4G 802.11g/b mixed.
- n-only** 2.4GHz 802.11n only.
- ngb-mixed** 2.4GHz 802.11n/b/g mixed.

Example

radio mode ngb-mixed

Syntax

radio band { 20 | 40 | 80 | auto }

Mode

Description

Set the wireless band.

Options

- 20** Standard - 20mhz channel.
- 40** Wide - 40mhz channel.
- 80** Wide - 80mhz channel.
- auto** Auto.

Example

radio band standard

Syntax

channel { primary <WIRELESS_CHANNEL> | secondary <WIRELESS_CHANNEL> | standard <WIRELESS_CHANNEL> }

Mode

Access Point

Description

Set the wireless channel.

Options

- primary** Set the wireless primary channel.
<WIRELESS_CHANNEL> Wireless channel.
Example: 9
- secondary** Set the wireless secondary channel.
<WIRELESS_CHANNEL> Wireless channel.
Example: 9
- standard** Set the wireless standard channel.
<WIRELESS_CHANNEL> Wireless channel.
Example: 9

Example

channel 8

Syntax

virtual-access-point group <WIRELESS_VAP_GROUP_NAME>

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless virtual access point group name.

Options

- <WIRELESS_VAP_GROUP_NAME>** Wireless VAP group name in the form: WORD or "QUOTED STRING".
Example: vapGroup

Example

virtual-access-point group CorpVAPGroup

Syntax

```
no virtual-access-point group
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Clear virtual access point group name.

Example

```
no virtual-access-point group
```

Syntax

```
wpa group-key update [ interval <UINT32> ]
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless WPA group key.

Options

update Set WPA group key update time.
interval Set WPA group key interval timeout in seconds.
<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

```
wpa group-key update  
wpa group-key update interval 86400
```

Syntax

```
no wpa group-key update
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable WPA group key update.

Options

update Disable WPA group key update.

Example

```
no wpa group-key update
```

Syntax

```
radius retries <UINT8>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless radius server retries.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
radius retries 4
```

Syntax

```
radius retry-interval <UINT8>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless radius server retry interval.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
radius retry-interval 20
```

Syntax

```
no radius retry-interval
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Clear wireless radius server retry interval.

Example

```
no radius retry-interval
```

Syntax

```
radius server { server1 | server2 } { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless radius sever configuration.

Options

server1	Server 1.
server2	Server 2.
ip	Set radius server IP.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
port	Set radius server port.
<IPV4_PORT>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
secret	Set radius server secret.
<ENC_PASSWORD>	Password. Example: <i>secret</i>

Example

```
radius server server1 ip 192.168.168.168
radius server server1 port 1812
radius server server1 secret radiusSec
```

Syntax

```
no radius server { server1 | server2 } { ip | port | secret }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Clear wireless radius sever configuration.

Options

server1	Server 1.
server2	Server 2.
ip	Set radius server IP.
port	Set radius server port.
secret	Set radius server secret.

Example

```
no radius server server1 ip
no radius server server1 port
no radius server server2 secret
```

Syntax

```
hide-ssid
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable hide SSID in beacon.

Example

hide-ssid

Syntax

no hide-ssid

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable hide SSID in beacon.

Example

no hide-ssid

Syntax

interval beacon <UINT16>

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless beacon interval in milliseconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

interval beacon 100

Syntax

green-ap enable

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable wireless green AP.

Example

greep-ap enable

Syntax

no green-ap enable

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable wireless green AP.

Example

```
no greep-ap enable
```

Syntax

```
green-ap timeout <UINT16>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless green AP timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
greep-ap timeout 200
```

Syntax

```
high-throughput { coexistence | encryption }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable wireless high throughput.

Options

coexistence Enable high throughput 20/40 coexistence.

encryption Enable high throughput rates with WEP or TKIP encryption method.

Example

```
high-throughput coexistence  
high-throughput encryption
```

Syntax

```
no high-throughput { coexistence | encryption }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable wireless high throughput.

Options

coexistence Disable high throughput 20/40 coexistence.

encryption Disable high throughput rates with WEP or TKIP encryption method.

Example

```
no high-throughput coexistence
no high-throughput encryption
```

Syntax

```
short-slot-time
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable short slot time.

Example

```
short-slot-time
```

Syntax

```
no short-slot-time
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable short slot time.

Example

```
no short-slot-time
```

Syntax

```
antenna-diversity best
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless antenna diversity.

Options

best Best.

Example

```
antenna-diversity best
```

Syntax

```
transmit-power { eighth | full | half | minimum | quarter }
```

Mode

Access Point
Wireless AccessPoint&Station
Wireless Bridge

Description

Set wireless transmit power.

Options

eighth Eighth (-9 db).

full Full power.

half Half (-3 db).

minimum Minimum.

quarter Quarter (-6 db).

Example

```
transmit-power minimum
```

Syntax

```
preamble-length { long | short }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless preamble length.

Options

long Long.

short Short.

Example

```
preamble-length long
```

Syntax

```
interval dtim <UINT8>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless DTIM interval.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interval dtim 1
```

Syntax

```
association-timeout <UINT16>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless association timeout in seconds.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
association-timeout 300
```

Syntax

```
max-clients <UINT8>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set wireless maximum client associations.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
max-clients 32
```

Syntax

```
data-rate <WIRELESS_RADIO_DATA_RATE>
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set data rate.

Options

<WIRELESS_RADIO_DATA_RATE> Wireless radio data rate.
Example: 36

Example

```
data-rate 48
```

Syntax

no protection mode

Mode

Access Point
Wireless AccessPoint&Station

Description

Clear wireless protection mode.

Example

no protection mode

Syntax

protection mode { always | auto }

Mode

Access Point
Wireless AccessPoint&Station

Description

Set the wireless protection mode.

Options

always Always.

auto Auto.

Example

protection mode none

Syntax

protection rate { 1 | 11 | 2 | 5 }

Mode

Access Point
Wireless AccessPoint&Station

Description

Set the wireless protection rate in mbps.

Options

1 1 Mbps

11 11 Mbps

2 2 Mbps

5 5 Mbps

Example

protection rate 5

Syntax

```
protection type { cts-only | rts-cts }
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Set the wireless protection type.

Options

cts-only Cts-only.

rts-cts RTS-CTS.

Example

```
protection type cts-only
```

Syntax

```
restore-default
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Restore advanced wireless settings to default.

Example

```
restore-default
```

Syntax

```
access-list [ allow { all | default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> } ] [ deny { default | group  
<ADDR_CUSTOM_GROUP_NAME_MIXED> } ]
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable/configure MAC filter lists.

Options

allow Set MAC filter allow list.

all All MAC addresses.

default Default wireless access list allow group.

group Name of access list allow group.

<ADDR_CUSTOM_GROUP_NAME_MIXED> Custom group address object name.
Example: *Sales Group*

deny Set MAC filter deny list.

default	Default wireless access list deny group.
group	Name of access list deny group.
<ADDR_CUSTOM_GROUP_NAME_MIXED>	Custom group address object name. Example: <i>Sales Group</i>

Example

```
access-list allow all
access-list allow all deny default
```

Syntax

```
no access-list [ deny ]
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable MAC filter list or clear deny access list.

Options

deny Clear deny access list.

Example

```
no access-list
no access-list deny
```

Syntax

```
wds
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Enable wireless distribution system.

Example

```
wds
```

Syntax

```
no wds
```

Mode

Access Point
Wireless AccessPoint&Station

Description

Disable wireless distribution system.

Example

```
no wds
```

Syntax

station

Mode

Wireless AccessPoint&Station

Description

Enter WLAN wireless station mode.

Example

station

Syntax

enable

Mode

Wireless Station Configuration

Description

Enable WLAN wireless station mode.

Example

enable

Syntax

no enable

Mode

Wireless Station Configuration

Description

Disable WLAN wireless station.

Example

no enable

Syntax

access-point ssid <WORD>

Mode

Wireless Station Configuration

Description

Set the access point SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

access-point ssid sonicwall

Syntax

```
no access-point ssid
```

Mode

Wireless Station Configuration

Description

Don't Set the access point SSID.

Example

```
no access-point ssid
```

Syntax

```
access-point authentication-type { open | wpa2 auto psk | wpa3 psk }
```

Mode

Wireless Station Configuration

Description

Set the access point authentication type.

Options

open WEP - open system.

wpa2 WPA2.

auto WPA2 - AUTO.

psk Wpa2 - AUTO - PSK.

wpa3 WPA3.

psk WPA3 - PSK.

Example

```
access-point authentication-type wpa2 auto psk
```

Syntax

```
access-point cipher-type { aes | tkip }
```

Mode

Wireless Station Configuration

Description

Set access point WPA cipher type.

Options

aes AES.

tkip TKIP.

Example

```
access-point cipher-type aes
```

Syntax

```
no access-point passphrase
```

Mode

Wireless Station Configuration

Description

Clear access point WPA passphrase.

Example

```
no access-point passphrase
```

Syntax

```
access-point passphrase <ENC_PASSWORD>
```

Mode

Wireless Station Configuration

Description

Set Access Point WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
access-point passphrase password
```

Syntax

```
no vlan-id
```

Mode

Wireless Station Configuration

Description

Clear station vlan id.

Example

```
no vlan-id
```

Syntax

```
vlan-id <STATION_VLAN_ID>
```

Mode

Wireless Station Configuration

Description

Set station vlan id.

Options

<STATION_VLAN_ID> VLAN ID.
Example: *100*

Example

```
vlan-id 100
```

Syntax

```
wireless-interface-as-wan
```

Mode

Wireless Station Configuration

Description

Enable wireless interface as WAN.

Example

```
wireless-interface-as-wan
```

Syntax

```
no wireless-interface-as-wan
```

Mode

Wireless Station Configuration

Description

Disable wireless interface as WAN.

Example

```
no wireless-interface-as-wan
```

Syntax

```
wds
```

Mode

Wireless Station Configuration

Description

Enable station wireless distribution system.

Example

```
wds
```

Syntax

```
no wds
```

Mode

Wireless Station Configuration

Description

Disable station wireless distribution system.

Example

```
no wds
```

Syntax

ids

Mode

Wireless

Description

Enter wireless IDS configuration mode.

Example

ids

Syntax

rogue-access-point-detection

Mode

Wireless IDS

Description

Enable rogue access point detection.

Example

rogue-access-point-detection

Syntax

no rogue-access-point-detection

Mode

Wireless IDS

Description

Disable rogue access point detection.

Example

no rogue-access-point-detection

Syntax

authorized-access-point { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }

Mode

Wireless IDS

Description

Set authorized access points.

Options

<i>all</i>	All authorized access points.

group	Specify MAC address object group for authorized access points.
<ADDR_CUSTOM_GROUP_NAME_MIXED>	Custom group address object name. Example: <i>Sales Group</i>

Example

```
authorized-access-point all
authorized-access-point group my-Authorized-ap-group
```

Syntax

```
schedule { days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

Wireless IDS

Description

Set the IDS schedule.

Options

days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule name "Work Hours"
```

Syntax

```
no schedule
```

Mode

Wireless IDS

Description

Clear the IDS schedule.

Example

```
no schedule
```

Syntax

```
authorizing-access-point mac <DETECTED_ACCESS_POINT_MAC>
```

Mode

Wireless IDS

Description

Authorizing the access point.

Options

<i>mac</i>	Specify access point MAC address.
<i><DETECTED_ACCESS_POINT_MAC></i>	Detected access point MAC address. Example: <i>00:0C:F1:56:98:AD</i>

Example

authorizing-access-point mac 00:19:D2:05:72:F4

Syntax

scan

Mode

Wireless IDS

Description

Run IDS scan.

Example

scan

Syntax

sonicpoint

Mode

Config

Description

Enter SonicPoint configuration mode.

Example

sonicpoint

Syntax

register sonicpoint <SONICPOINT_N_NAME> country-code <SONICPOINT_N_REGISTER_COUNTRY_CODE>

Mode

SonicPoint

Description

Register SonicPoint with specified country code.

Options

<i><SONICPOINT_N_NAME></i>	SonicPointN name. Example: <i>mySonicpointn</i>
<i>country-code</i>	SonicPoint country code.
<i><SONICPOINT_N_REGISTER_COUNTRY_CODE></i>	SonicPointN register country code. Example: <i>United States</i>

Example

register sonicpoint "SonicPointN 2e57e" country-code "United States"

Syntax

firmware-management

Mode

SonicPoint

Description

Enter SonicPoint firmware management mode.

Example

firmware-management

Syntax

override-download-url sonicpoint n <WORD>

Mode

SonicPoint Firmware Management

Description

Manually specify SonicPoint N image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

override-download-url sonicpoint n my.webserver.local/applications/sonicpointn.img.bin

Syntax

no override-download-url sonicpoint n

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicPoint N image URL.

Example

no override-download-url sonicpoint n

Syntax

override-download-url sonicpoint nv <WORD>

Mode

SonicPoint Firmware Management

Description

Manually specify SonicPoint Ni/Ne image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicpoint nv my.webserver.local/applications/sonicpointnv.img.bin
```

Syntax

```
no override-download-url sonicpoint nv
```

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicPoint Ni/Ne image URL.

Example

```
no override-download-url sonicpoint nv
```

Syntax

```
override-download-url sonicpoint ndr <WORD>
```

Mode

SonicPoint Firmware Management

Description

Manually specify SonicPoint NDR image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicpoint ndr my.webserver.local/applications/sonicpointndr.img.bin
```

Syntax

```
no override-download-url sonicpoint ndr
```

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicPoint NDR image URL.

Example

```
no override-download-url sonicpoint ndr
```

Syntax

```
override-download-url sonicpoint ac <WORD>
```

Mode

SonicPoint Firmware Management

Description

Manually specify SonicPoint AC image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicpoint ac my.webserver.local/applications/sonicpointac.img.bin
```

Syntax

```
no override-download-url sonicpoint ac
```

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicPoint AC image URL.

Example

```
no override-download-url sonicpoint ac
```

Syntax

```
override-download-url sonicwave400 <WORD>
```

Mode

SonicPoint Firmware Management

Description

Manually specify SonicWave-432o/432i/432e image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicwave400 my.webserver.local/applications/sonicpointac.img.bin
```

Syntax

```
no override-download-url sonicwave400
```

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicWave-432o/432i/432e image URL.

Example

```
no override-download-url sonicwave400
```

Syntax

```
override-download-url sonicwave200 <WORD>
```

Mode

SonicPoint Firmware Management

Description

Manually specify SonicWave-231c/224w/231o image URL (http://).

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
override-download-url sonicwave200 my.webserver.local/applications/sonicpointac.img.bin
```

Syntax

```
no override-download-url sonicwave200
```

Mode

SonicPoint Firmware Management

Description

Disable manually specifying SonicWave-231c/224w/231o image URL.

Example

```
no override-download-url sonicwave200
```

Syntax

```
reset sonicpoint
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicPoint.

Example

```
reset sonicpoint
```

Syntax

```
reset sonicpoint-n
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicPoint-N.

Example

```
reset sonicpoint-n
```

Syntax

```
reset sonicpoint-nv
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicPoint-Ni/Ne.

Example

```
reset sonicpoint-nv
```

Syntax

```
reset sonicpoint-ndr
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicPoint-NDR.

Example

```
reset sonicpoint-ndr
```

Syntax

```
reset sonicpoint-ac
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicPoint-ACe/ACi/N2.

Example

```
reset sonicpoint-ac
```

Syntax

```
reset sonicwave400
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicWave-432o/432i/432e.

Example

```
reset sonicwave400
```

Syntax

```
reset sonicwave200
```

Mode

SonicPoint Firmware Management

Description

Reset the firmware image SonicWave-231c/224w/231o.

Example

```
reset sonicwave200
```

Syntax

```
upload sonicpoint
```

Mode

SonicPoint Firmware Management

Description

upload the firmware image of SonicPoint.

Example

```
upload sonicpoint
```

Syntax

```
upload sonicpoint-n
```

Mode

SonicPoint Firmware Management

Description

upload the firmware image of SonicPoint-N.

Example

```
upload sonicpoint-n
```

Syntax

```
upload sonicpoint-nv
```

Mode

SonicPoint Firmware Management

Description

Upload the firmware image SonicPoint-Ni/Ne.

Example

```
upload sonicpoint-nv
```

Syntax

```
upload sonicpoint-ndr
```

Mode

SonicPoint Firmware Management

Description

Upload the firmware image SonicPoint-NDR.

Example

```
upload sonicpoint-ndr
```

Syntax

```
upload sonicpoint-ac
```

Mode

SonicPoint Firmware Management

Description

Upload the firmware image SonicPoint-ACe/ACi/N2.

Example

```
upload sonicpoint-ac
```

Syntax

```
upload sonicwave400
```

Mode

SonicPoint Firmware Management

Description

Upload the firmware image SonicWave-432o/432i/432e.

Example

```
upload sonicwave400
```

Syntax

```
upload sonicwave200
```

Mode

SonicPoint Firmware Management

Description

Upload the firmware image SonicWave-231c/224w/231o.

Example

```
upload sonicwave200
```

Syntax

```
synchronize
```

Mode

SonicPoint

Description

Synchronize SonicPoints and SonicPointNs.

Example

synchronize

Syntax

reboot { sonicpoint [ac | n | ndr | wave2] <SONICPOINT_N_NAME> | sonicpoints } [factory-default]

Mode

SonicPoint

Description

Reboot specified SonicPoint or all SonicPoints.

Options

sonicpoint	Specify SonicPoint.
ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
sonicpoints	Reboot all SonicPoints.
factory-default	Reboot to factory default.

Example

reboot sonicpoint "SonicPointN 2e57e"

Syntax

no sonicpoint [ac | n | ndr | wave2] <SONICPOINT_N_NAME>

Mode

SonicPoint

Description

Delete or disable the specified SonicPoint.

Options

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>

Example

no sonicpoint n "SonicPointN 2e57e"
no sonicpoint "SonicPointN 2e57e"

Syntax

```
no profile [ ac | n | ndr | wave2 ] <SONICPOINT_N_PROFILE_NAME>
```

Mode

SonicPoint

Description

Delete SonicPoint provisioning profile.

Options

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2 profile.
<SONICPOINT_N_PROFILE_NAME>	SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i>

Example

```
no profile n CorpSonic
no profile CorpSonic
```

Syntax

```
no sonicpoints [ { ac | n | ndr | wave2 } ]
```

Mode

SonicPoint

Description

Delete all SonicPoints.

Options

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2.

Example

```
no sonicpoints
no sonicpoints n
```

Syntax

```
no profiles [ { ac | n | ndr | wave2 } ]
```

Mode

SonicPoint

Description

Delete all SonicPoint provisioning profiles.

Options

- ac** SonicPoint ACe/ACi/N2/W2.
- n** SonicPoint N.
- ndr** SonicPoint NDR.
- wave2** SonicPoint ACWave2.

Example

```
no profiles
no profiles n
```

Syntax

```
sonicpoint { ac | n | ndr | wave2 } <SONICPOINT_N_NAME>
```

Mode

SonicPoint

Description

Edit SonicPoint and enter its configuration mode.

Options

- ac** SonicPoint ACe/ACi/N2/W2.
- n** SonicPoint N.
- ndr** SonicPoint NDR.
- wave2** SonicPoint ACWave2.
- <SONICPOINT_N_NAME>** SonicPointN name.
Example: *mySonicpointn*

Example

```
sonicpoint n "SonicPointN 2e57e"
```

Syntax

```
profile { ac | n | ndr | wave2 } <SONICPOINT_N_PROFILE_NAME>
```

Mode

SonicPoint

Description

Add/edit SonicPoint provisioning profile and enter its configuration mode.

Options

- ac** SonicPoint ACe/ACi/N2/W2.
- n** SonicPoint N.
- ndr** SonicPoint NDR.
- wave2** SonicPoint ACWave2.
- <SONICPOINT_N_PROFILE_NAME>** SonicPointN provisioning profile name.

Example: *mySonicpointnProfile*

Example

```
profile n CorpSonic
```

Syntax

```
enable
```

Mode

SonicPointN

Description

Enable SonicPointN.

Example

```
enable
```

Syntax

```
no enable
```

Mode

SonicPointN

Description

Disable SonicPointN.

Example

```
no enable
```

Syntax

```
rf-monitoring
```

Mode

SonicPointN

Description

Enable RF monitoring.

Example

```
rf-monitoring
```

Syntax

```
no rf-monitoring
```

Mode

SonicPointN

Description

Disable RF monitoring.

Example

```
no rf-monitoring
```

Syntax

```
poe-out
```

Mode

SonicPointN

Description

Enable POE out.

Example

```
poe-out
```

Syntax

```
no poe-out
```

Mode

SonicPointN

Description

Disable POE out.

Example

```
no poe-out
```

Syntax

```
low-power
```

Mode

SonicPointN

Description

Enable low power mode.

Example

```
low-power
```

Syntax

```
no low-power
```

Mode

SonicPointN

Description

Disable low power mode.

Example

```
no low-power
```

Syntax

```
retain [ all | led | radio [ 2400mhz | 5000mhz | single-radio ] [ { access-list | advanced | radio-settings | virtual-access-point | wireless-security } ] | retain | rf-monitoring | sonicpoint [ { access-point | ip | name-and-country-code } ] | widp-sensor ]
```

Mode

SonicPointN

Description

Enable retain settings.

Options

all	Retain all settings.
led	Retain enable LED(Ni/Ne only).
radio	Retain radio settings.
2400mhz	Retain 2.4GHz radio settings.
5000mhz	Retain 5GHz radio settings.
single-radio	Retain radio settings.
access-list	Retain access list enforcement.
advanced	Retain advanced radio settings.
radio-settings	Retain radio settings.
virtual-access-point	Retain virtual access point settings.
wireless-security	Retain wireless security settings.
retain	Retain enable retain settings
rf-monitoring	Retain enable RF monitoring.
sonicpoint	Retain enable SonicPoint.
access-point	Retain enable access point.
ip	Retain SonicPoint IP information.
name-and-country-code	Retain SonicPoint name and country code.
widp-sensor	Retain DIDP sensor.

Example

```
retain all
retain retain
retain sonicpoint
retain sonicpoint name-and-country-code
retain radio
retain radio advanced
```

Syntax

```
no retain [ all | led | radio [ 2400mhz | 5000mhz | single-radio ] [ { access-list | advanced | radio-settings | virtual-access-point | wireless-security } ] | retain | rf-monitoring | sonicpoint [ { access-point | ip | name-and-country-code } ] |
```

Mode

SonicPointN

Description

Disable SonicPointN retain settings.

Options

all	Retain all settings.
led	Retain enable LED(Ni/Ne only).
radio	Retain radio settings.
2400mhz	Retain 2.4GHz radio settings.
5000mhz	Retain 5GHz radio settings.
single-radio	Retain radio settings.
access-list	Retain access list enforcement.
advanced	Retain advanced radio settings.
radio-settings	Retain radio settings.
virtual-access-point	Retain virtual access point settings.
wireless-security	Retain wireless security settings.
retain	Retain enable retain settings
rf-monitoring	Retain enable RF monitoring.
sonicpoint	Retain enable SonicPoint.
access-point	Retain enable access point.
ip	Retain SonicPoint IP information.
name-and-country-code	Retain SonicPoint name and country code.
widp-sensor	Retain DIDP sensor.

Example

```
no retain
no retain retain
no retain sonicpoint
no retain sonicpoint name-and-country-code
no retain radio
no retain radio advanced
```

Syntax

```
led
```

Mode

SonicPointN

Description

Enable SonicPointN LED.

Example

```
led
```

Syntax

```
no led
```

Mode

SonicPointN

Description

Disable SonicPointN LED.

Example

```
no led
```

Syntax

```
name-prefix <WORD>
```

Mode

SonicPointN

Description

Set provisioning profile name prefix.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name-prefix CorpSonicPointN
```

Syntax

```
name <WORD>
```

Mode

SonicPointN

Description

Set SonicPointN name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
name CorpSonicPointN-1234
```

Syntax

```
country-code <SONICPOINT_N_COUNTRY_CODE>
```

Mode

SonicPointN

Description

Set SonicPointN country code.

Options

<SONICPOINT_N_COUNTRY_CODE> SonicPointN country code.
Example: *United States*

Example

country-code "United States"

Syntax

eapol-version { v1 | v2 }

Mode

SonicPointN

Description

Set EAPOL version (v2 provides better security).

Options

v1 Version 1.

v2 Version 2.

Example

eapol-version v2

Syntax

band-steering { auto | force-5ghz | prefer-5ghz }

Mode

SonicPointN

Description

Set band steering.

Options

auto Auto.

force-5ghz Force 5GHz.

prefer-5ghz Prefer 5GHz.

Example

band-steering auto

Syntax

no band-steering

Mode

SonicPointN

Description

Disable band steering.

Example

no band-steering

Syntax

sslvpn { auto-reconnect | domain <HOSTNAME_MIXED> | password <ENC_PASSWORD> | server <WORD> | user-name <WORD> }

Mode

SonicPointN

Description

Set SonicPoint L3 SSLVPN tunnel.

Options

<i>auto-reconnect</i>	Enable SonicPoint L3 SSLVPN tunnel auto reconnect.
<i>domain</i> <i><HOSTNAME_MIXED></i>	Set SonicPoint L3 SSLVPN tunnel user domain. IPv4: hostname in the form: D.D.D.D or hostname\nIPv6: host address in the form: HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH:HHHH\n. Example: <i>2001:cdba:0000:0000:0000:0000:3257:9652\n</i>
<i>password</i> <i><ENC_PASSWORD></i>	Set SonicPoint L3 SSLVPN tunnel user password. Password. Example: <i>secret</i>
<i>server</i> <i><WORD></i>	Set SonicPoint L3 SSLVPN tunnel server. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>user-name</i> <i><WORD></i>	Set SonicPoint L3 SSLVPN tunnel user name. Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

*sslvpn server 172.168.12.4
sslvpn user-name jshone
sslvpn password password
sslvpn domain mySonicPoint.com
sslvpn auto-reconnect*

Syntax

no sslvpn { auto-reconnect | domain | password | server | user-name }

Mode

SonicPointN

Description

Clear SonicPoint L3 SSLVPN tunnel settings.

Options

<i>auto-reconnect</i>	Disable SonicPoint L3 SSLVPN tunnel auto reconnect.

domain	Clear SonicPoint L3 SSLVPN tunnel user domain.
password	Clear SonicPoint L3 SSLVPN tunnel user password.
server	Clear SonicPoint L3 SSLVPN tunnel server.
user-name	Clear SonicPoint L3 SSLVPN tunnel user name.

Example

```
no sslvpn server
no sslvpn user-name
no sslvpn password
no sslvpn domain
no sslvpn auto-reconnect
```

Syntax

```
radius { accounting { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } | nas { {
identifier { { sonicpoint-mac-address | sonicpoint-name | sonicpoint-ssid } } | ip <IPV4_HOST> } } | retries <UINT8> | retry-
interval <UINT8> | server { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } }
```

Mode

SonicPointN

Description

Set radius server for SonicPoint radio.

Options

accounting	Set radius accounting server.
server1	Radius accounting server 1.
server2	Radius accounting server 2.
ip <IPV4_HOST>	Radius accounting server IP. IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
port <IPV4_PORT>	Radius accounting server port. Integer in the form: D OR 0xHHHH. Example: <i>80</i>
secret <ENC_PASSWORD>	Radius accounting server secret. Password. Example: <i>secret</i>
nas	Nas settings to radius server.
identifier	Nas identifier to radius server.
sonicpoint-mac-address	SonicPoint's MAC address.
sonicpoint-name	SonicPoint's name.
sonicpoint-ssid	SonicPoint's SSID.
ip <IPV4_HOST>	Nas IP to radius server. IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
retries <UINT8>	Set radius server retries. Integer in the form: D OR 0xHH. Example: <i>123</i>

<i>retry-interval</i> <UINT8>	Set radius server retry interval (seconds). Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>server</i>	Set radius server.
<i>server1</i>	Radius server 1.
<i>server2</i>	Radius server 2.
<i>ip</i> <IPV4_HOST>	Radius server IP. IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>port</i> <IPV4_PORT>	Radius server port. Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>secret</i> <ENC_PASSWORD>	Radius server secret. Password. Example: <i>secret</i>

Example

```
radius retries 1
radius retry-interval 20
radius server server1 ip 192.168.168.1
radius server server1 port 1812
radius server server1 secret radsecret
radius server server2 ip 192.168.168.2
radius server server2 port 1812
radius server server2 secret radsecret2
radius accounting server1 ip 192.168.168.1
radius accounting server1 port 1812
radius accounting server1 secret radsecret
radius accounting server2 ip 192.168.168.2
radius accounting server2 port 1812
radius accounting server2 secret radsecret2
radius nas identifier sonicpoint-name
radius nas identifier sonicpoint-mac-address
```

Syntax

```
no radius { accounting { server1 | server2 } { { ip | port | secret } } | nas { { identifier | ip } } | retries | retry-
interval | server { server1 | server2 } { { ip | port | secret } } }
```

Mode

SonicPointN

Description

Clear radius server settings for SonicPoint radio.

Options

<i>accounting</i>	Clear radius accounting server settings.
<i>server1</i>	Clear radius accounting server 1 settings.
<i>server2</i>	Clear radius accounting server 2 settings.
<i>ip</i>	Clear radius accounting server IP.
<i>port</i>	Clear radius accounting server port.
<i>secret</i>	Clear radius accounting server secret.
<i>nas</i>	Clear nas settings to radius server.
<i>identifier</i>	Nas identifier to radius server not included.

ip	Clear nas IP to radius server.
retries	Clear radius server retries.
retry-interval	Clear radius server retry interval.
server	Clear radius server settings.
server1	Clear radius server 1 settings.
server2	Clear radius server 2 settings.
ip	Clear radius server IP.
port	Clear radius server port.
secret	Clear radius server secret.

Example

```
no radius retries
no radius retry-interval
no radius server server1 ip
no radius server server1 port
no radius server server1 secret
no radius server server2 ip
no radius server server2 port
no radius server server2 secret
no radius accouting server1 ip
no radius accouting server1 port
no radius accouting server1 secret
no radius accouting server2 ip
no radius accouting server2 port
no radius accouting server2 secret
no radius nas identifier
```

Syntax

```
administrator { name <WORD> | password <ENC_PASSWORD> }
```

Mode

SonicPointN

Description

Set SonicPoint administrator name or password.

Options

name	Set SonicPoint administrator name.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
password	Set SonicPoint administrator password.
<ENC_PASSWORD>	Password. Example: <i>secret</i>

Example

```
administrator name admin
administrator password password
```

Syntax

```
no administrator { name | password }
```

Mode

SonicPointN

Description

Clear SonicPoint administrator name or password.

Options

- name** Clear SonicPoint administrator name.
- password** Clear SonicPoint administrator password.

Example

```
no administrator name
no administrator password
```

Syntax

```
widp-sensor schedule { always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

SonicPointN

Description

Enable WIDP sensor and set WIDP sensor schedule.

Options

- schedule** Set WIDP sensor schedule.
- always-on** Always on.
- days** Schedule object days.
<SCHED_DAYS> Days of the week in the form: SU-M-T-W-TH-F-SA.
Example: *SU-M-TH-SA*
- time** Schedule object beginning/ending time.
<SCHED_TIME_BEGIN> Time in the form: DD:DD.
Example: *12:00*
<SCHED_TIME_END> Time in the form: DD:DD.
Example: *12:00*
- name** Schedule object name.
<SCHED_NAME> Schedule object name.
Example: *Work Hours*

Example

```
widp-sensor schedule name "Work Hours"
```

Syntax

```
no widp-sensor
```

Mode

SonicPointN

Description

Disable WIDP sensor.

Example

```
no widp-sensor
```

Syntax

```
wwan { bound-to <SONICPOINT_WWAN_VLAN_INTERFACE> | enable }
```

Mode

SonicPointN

Description

Set SonicPoint 3G/4G WWAN.

Options

bound-to Set SonicPoint 3G/4G WWAN bound to WAN VLAN interface.
<SONICPOINT_WWAN_VLAN_INTERFACE> SonicPoint WWAN VLAN interface name.
Example: *X2:253*

enable Enable SonicPoint 3G/4G WWAN.

Example

```
wwan enable
wwan bound-to X2:V33
```

Syntax

```
no wwan { bound-to | enable }
```

Mode

SonicPointN

Description

Disable SonicPoint 3G/4G WWAN.

Options

bound-to clear SonicPoint 3G/4G WWAN bound to WAN VLAN interface.

enable Disable SonicPoint 3G/4G WWAN.

Example

```
no wwan enable
no wwan bound-to
```

Syntax

```
connection-profile
```

Mode

SonicPointN

Description

Set SonicPoint 3G/4G WWAN connection profile configuration.

Example

```
connection-profile
```

Syntax

enable

Mode

WWAN Profile

Description

Enable SonicPoint 3G/4G WWAN connection profile.

Example

enable

Syntax

no enable

Mode

WWAN Profile

Description

Disable SonicPoint 3G/4G WWAN connection profile.

Example

no enable

Syntax

country <WORD>

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile country.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

country usa

Syntax

no country

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile country.

Example

no country

Syntax

```
service-provider <WORD>
```

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile provider.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
service-provider sprint
```

Syntax

```
no service-provider
```

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile provider.

Example

```
no service-provider
```

Syntax

```
plan-type <WORD>
```

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile plan type.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
plan-type standard
```

Syntax

```
no plan-type
```

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile plan type.

Example

```
no plan-type
```

Syntax

```
connection-type { cdma-evdo | gprs-hspa-lte }
```

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile connection type.

Options

cdma-evdo CDMA/EVDO.

gprs-hspa-lte GPRS/HSPA/LTE.

Example

```
connection-type cdma-evdo
```

Syntax

```
no connection-type
```

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile connection type.

Example

```
no connection-type
```

Syntax

```
dial-number <WORD>
```

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile dialed number.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
dial-number #777
```

Syntax

no dialed-number

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile dialed number.

Example

no dialed-number

Syntax

user-name <WORD>

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile user name.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

user-name guest

Syntax

no user-name

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile user name.

Example

no user-name

Syntax

user-password <ENC_PASSWORD>

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile user password.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

user-password password

Syntax

no user-password

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile user password.

Example

no user-password

Syntax

apn <WORD>

Mode

WWAN Profile

Description

Set SonicPoint 3G/4G WWAN connection profile apn.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

apn i.spsn

Syntax

no apn

Mode

WWAN Profile

Description

Clear SonicPoint 3G/4G WWAN connection profile apn.

Example

no apn

Syntax

mesh { 2400mhz | 5000mhz } [enable | psk <ENC_PASSWORD> | rssi-threshold <INT16> | ssid <WORD>]

Mode

SonicPointN

Description

Set sonicwave MESH network.

Options

2400mhz	Set sonicwave MESH in radio 2.4GHz.
5000mhz	Set sonicwave MESH in radio 5GHz.
enable	Enable sonicwave MESH
psk	Set sonicwave MESH psk.
<ENC_PASSWORD>	Password. Example: <i>secret</i>
rssi-threshold	Set sonicwave MESH rssi-threshold.
<INT16>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
ssid	Set sonicwave MESH ssid.
<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
mesh 2400mhz
mesh 2400mhz ssid SonicWave_Mesh
mesh 2400mhz psk password
mesh 2400mhz rssi-threshold -80
```

Syntax

```
no mesh { 2400mhz | 5000mhz } [ enable | psk | ssid ]
```

Mode

SonicPointN

Description

Clear sonicwave MESH network.

Options

2400mhz	Disable sonicwave MESH in radio 2.4GHz.
5000mhz	Disable sonicwave MESH in radio 5GHz.
enable	Disable sonicwave MESH.
psk	Clear sonicwave MESH psk.
ssid	Clear sonicwave MESH ssid.

Example

```
no mesh 2400mhz
no mesh 2400mhz ssid
no mesh 2400mhz psk
```

Syntax

```
ble { advertisement | ibeacon { enable | major <UINT16> | minor <UINT16> | uuid <SONICPOINT_BLE_IBEACON_UUID> } }
```

Mode

SonicPointN

Description

Set SonicWave Bluetooth Low Energy.

Options

<i>advertisement</i>	Enable SonicWave Bluetooth Advertisement.
<i>ibeacon</i>	SonicWave Bluetooth Low Energy iBeacon.
<i>enable</i>	Enable SonicWave BLE iBeacon.
<i>major</i> <UINT16>	Set SonicWave BLE iBeacon major. Integer in the form: D OR 0xHHHH. Example: 123
<i>minor</i> <UINT16>	Set SonicWave BLE iBeacon minor. Integer in the form: D OR 0xHHHH. Example: 123
<i>uuid</i> <SONICPOINT_BLE_IBEACON_UUID>	Set SonicWave BLE iBeacon UUID. SonicWave BLE iBeacon UUID. Example: 51b9d455-6a32-426c-b5cc-524181c24df3

Example

```
ble advertisement
ble ibeacon enable
ble ibeacon uuid 51b9d455-6a32-426c-b5cc-524181c24df3
ble ibeacon major 4
ble ibeacon minor 3
```

Syntax

```
no ble { advertisement | ibeacon { enable | major | minor | uuid } }
```

Mode

SonicPointN

Description

Disable SonicWave Bluetooth Low Energy.

Options

<i>advertisement</i>	Disable SonicWave BLE Advertisement.
<i>ibeacon</i>	SonicWave BLE iBeacon.
<i>enable</i>	Disable SonicWave BLE iBeacon.
<i>major</i>	Clear SonicWave BLE iBeacon major.
<i>minor</i>	Clear SonicWave BLE iBeacon minor.
<i>uuid</i>	Clear SonicWave BLE iBeacon UUID.

Example

```
no ble ibeacon enable
```

Syntax

```
packet-capture
```

Mode

SonicPointN

Description

Configuration SonicPoint packet capture and enter its configuration mode.

Example

```
packet-capture
```

Syntax

```
mode { 2400mhz { { ngb-mixed } } | 5000mhz { { ac-na-mixed | na-mixed } } }
```

Mode

Capture Radio

Description

Set the capture radio mode.

Options

2400mhz	2.4GHz.
ngb-mixed	2.4GHz 802.11n/b/g mixed.
5000mhz	5GHz.
ac-na-mixed	5GHz 802.11ac/n/a mixed.
na-mixed	5GHz 802.11n/a mixed.

Example

```
mode 2400mhz ngb-mixed
mode 5000mhz na-mixed
```

Syntax

```
band { 20 | 40 | 80 }
```

Mode

Capture Radio

Description

Set the capture radio band.

Options

20	Standard - 20mhz channel.
40	Wide - 40mhz channel.
80	Wide - 80mhz channel.

Example

```
band 20
```

Syntax

```
channel { primary <SONICPOINT_N_CAPTURE_CHANNEL> | secondary <SONICPOINT_N_CAPTURE_CHANNEL> | standard <SONICPOINT_N_CAPTURE_CHANNEL> }
```

Mode

Capture Radio

Description

Set the capture radio channel.

Options

<i>primary</i>	Set the radio primary channel.
<i><SONICPOINT_N_CAPTURE_CHANNEL></i>	SonicPointN capture channel. Example: 6
<i>secondary</i>	Set the radio secondary channel.
<i><SONICPOINT_N_CAPTURE_CHANNEL></i>	SonicPointN capture channel. Example: 6
<i>standard</i>	Set the radio standard channel.
<i><SONICPOINT_N_CAPTURE_CHANNEL></i>	SonicPointN capture channel. Example: 6

Example

channel auto

Syntax

capture [bidirectional | exclude [{ beacon | control | data | probe [{ request | response }] }] | packet-capture | wrap-buffer]

Mode

Capture Radio

Description

Enable capture settings.

Options

<i>bidirectional</i>	Enable bidirectional address matching.
<i>exclude</i>	EXCLUDE.
<i>beacon</i>	Exclude beacon.
<i>control</i>	Exclude control.
<i>data</i>	Exclude data.
<i>probe</i>	PROBE.
<i>request</i>	Exclude probe request.
<i>response</i>	Exclude probe response.
<i>packet-capture</i>	Enable packet capture.
<i>wrap-buffer</i>	Wrap capture buffer once full.

Example

*capture wrap-buffer
capture bidirectional
capture exclude beacon
capture exclude probe request
capture exclude probe response
capture exclude control
capture exclude data*

Syntax

```
no capture [ bidirectional | exclude [ { beacon | control | data | probe [ { request | response } ] } ] | packet-capture | wrap-buffer ]
```

Mode

Capture Radio

Description

Disable capture settings.

Options

<i>bidirectional</i>	Enable bidirectional address matching.
<i>exclude</i>	EXCLUDE.
<i>beacon</i>	Exclude beacon.
<i>control</i>	Exclude control.
<i>data</i>	Exclude data.
<i>probe</i>	PROBE.
<i>request</i>	Exclude probe request.
<i>response</i>	Exclude probe response.
<i>packet-capture</i>	Enable packet capture.
<i>wrap-buffer</i>	Wrap capture buffer once full.

Example

```
no capture
no capture wrap-buffer
no capture bidirectional
no capture exclude beacon
no capture exclude probe request
no capture exclude probe response
no capture exclude control
no capture exclude data
```

Syntax

```
ssid <WORD>
```

Mode

Capture Radio

Description

Set the capture ESSID.

Options

<WORD>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>

Example

```
ssid sonicwall
```

Syntax

no essid

Mode

Capture Radio

Description

Clear capture ESSID.

Example

no essid

Syntax

bssid <ADDR_MAC>

Mode

Capture Radio

Description

Set the capture BSSID.

Options

<ADDR_MAC> Address object MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.

Example

bssid 18:b1:69:4d:28:c0

Syntax

no bssid

Mode

Capture Radio

Description

Clear capture BSSID.

Example

no bssid

Syntax

mac { destination <SONICPOINT_CAPTURE_MAC> | source <SONICPOINT_CAPTURE_MAC> }

Mode

Capture Radio

Description

Set the capture source or destination MAC address(es).

Options

destination Set the capture destination MAC address(es).
<SONICPOINT_CAPTURE_MAC> SonicPoint capture filter MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.\n You can

enter up to five MAC at most with separated by commas or space.

source

Set the capture source MAC address(es).

<SONICPOINT_CAPTURE_MAC>

SonicPoint capture filter MAC address in the form: HH:HH:HH:HH:HH:HH or HHHHHHHHHHHH or HH-HH-HH-HH-HH-HH.\n You can enter up to five MAC at most with separated by commas or space.

Example

```
mac source 18:b1:69:4d:28:c0,c0:ea:e4:a7:57:c4
```

Syntax

```
no mac { destination | source }
```

Mode

Capture Radio

Description

Clear capture source or destination MAC address(es).

Options

destination Clear the capture destination MAC address(es).

source Clear the capture source MAC address(es).

Example

```
no mac source
```

Syntax

```
radio
```

Mode

SonicPointN

Description

Configuration SonicPoint radio and enter its configuration mode.

Example

```
radio
```

Syntax

```
radio-2400mhz
```

Mode

SonicPointN

Description

Configuration SonicPoint radio 2.4GHz and enter its configuration mode.

Example

```
radio-2400mhz
```

Syntax

```
radio-5000mhz
```

Mode

SonicPointN

Description

Configuration SonicPoint radio 5GHz and enter its configuration mode.

Example

```
radio-5000mhz
```

Syntax

```
virtual-access-point group <VAP_GROUP>
```

Mode

Radio N
Radio 2.4GHz

Description

Set virtual access point group name.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
virtual-access-point group CorpAccess
```

Syntax

```
no virtual-access-point group
```

Mode

Radio N
Radio 2.4GHz

Description

Clear virtual access point group name.

Example

```
no virtual-access-point group
```

Syntax

```
dynamic-vlan
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint dynamic vlan assignment id for radio.

Example

dynamic-vlan

Syntax

no dynamic-vlan

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint dynamic vlan assignment id for radio.

Example

no dynamic-vlan

Syntax

vlan <VAP_VLAN_ID>

Mode

Radio N
Radio 2.4GHz

Description

Set SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

vlan 4

Syntax

no vlan <VAP_VLAN_ID>

Mode

Radio N
Radio 2.4GHz

Description

Clear SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

no vlan 4

Syntax

no vlans

Mode

Radio N
Radio 2.4GHz

Description

Clear SonicPoint dynamic VLAN IDs.

Example

no vlans

Syntax

enable

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint radio.

Example

enable

Syntax

no enable

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint radio.

Example

no enable

Syntax

schedule [always-on | days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME>]

Mode

Radio N
Radio 2.4GHz

Description

Set schedule for radio.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<i><SCHED_DAYS></i>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<i><SCHED_TIME_BEGIN></i>	Time in the form: DD:DD.

<SCHED_TIME_END>	Example: <i>12:00</i> Time in the form: DD:DD. Example: <i>12:00</i>
name	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

```
schedule name "Work Hours"
```

Syntax

```
mode { 5000mhz { { a-only | ac-na-mixed | ac-only | n-only | na-mixed } } | g-only | n-only | ngb-mixed }
```

Mode

Radio N
Radio 2.4GHz

Description

Set the radio mode.

Options

5000mhz	5GHz.
a-only	5GHz 802.11a only.
ac-na-mixed	5GHz 802.11ac/n/a mixed.
ac-only	5GHz 802.11ac only.
n-only	5GHz 802.11n only.
na-mixed	5GHz 802.11n/a mixed.
g-only	2.4GHz 802.11g only.
n-only	2.4GHz 802.11n only.
ngb-mixed	2.4GHz 802.11n/b/g mixed.

Example

```
mode ngb-mixed
mode 5000mhz na-mixed
```

Syntax

```
dfs-channel
```

Mode

Radio N

Description

Enable DFS channel.

Example

```
dfs-channel
```

Syntax

```
no dfs-channel
```

Mode

Radio N

Description

Disable DFS channel.

Example

```
no dfs-channel
```

Syntax

```
ssid <WORD>
```

Mode

Radio N

Radio 2.4GHz

Description

Set the radio SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ssid sonicwall
```

Syntax

```
no ssid
```

Mode

Radio N

Radio 2.4GHz

Description

Clear the radio SSID.

Example

```
no ssid
```

Syntax

```
channel { primary <SONICPOINT_N_CHANNEL> | secondary <SONICPOINT_N_CHANNEL> | standard <SONICPOINT_N_CHANNEL> }
```

Mode

Radio N

Radio 2.4GHz

Description

Set the radio channel.

Options

primary	Set the radio primary channel.
<SONICPOINT_N_CHANNEL>	SonicPointN channel. Example: <i>auto</i>
secondary	Set the radio secondary channel.
<SONICPOINT_N_CHANNEL>	SonicPointN channel. Example: <i>auto</i>
standard	Set the radio standard channel.
<SONICPOINT_N_CHANNEL>	SonicPointN channel. Example: <i>auto</i>

Example

channel primary auto

Syntax

band { 20 | 40 | 80 | auto }

Mode

Radio N
Radio 2.4GHz

Description

Set the radio band.

Options

- 20** Standard - 20mhz channel.
- 40** Wide - 40mhz channel.
- 80** Wide - 80mhz channel.
- auto** Auto.

Example

band standard

Syntax

short-guard-interval

Mode

Radio N
Radio 2.4GHz

Description

Enable short guard interval.

Example

short-guard-interval

Syntax

no short-guard-interval

Mode

Radio N
Radio 2.4GHz

Description

Disable short guard interval.

Example

```
no short-guard-interval
```

Syntax

```
aggregation
```

Mode

Radio N
Radio 2.4GHz

Description

Enable aggregation.

Example

```
aggregation
```

Syntax

```
no aggregation
```

Mode

Radio N
Radio 2.4GHz

Description

Disable aggregation.

Example

```
no aggregation
```

Syntax

```
mimo
```

Mode

Radio N
Radio 2.4GHz

Description

Enable MIMO.

Example

```
mimo
```

Syntax

```
no mimo
```

Mode

Radio N
Radio 2.4GHz

Description

Disable MIMO.

Example

no mimo

Syntax

no access-list [deny]

Mode

Radio N
Radio 2.4GHz

Description

Disable MAC filter list or set no deny access list.

Options

deny Set no deny access list.

Example

no access-list
no access-list deny

Syntax

access-list [allow { all | default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }] [deny { default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }]

Mode

Radio N
Radio 2.4GHz

Description

Enable/configure MAC filter lists.

Options

- allow**Set MAC filter allow list.
- all**All MAC addresses.
- default**Default SonicPoint ACL allow group.
- group**Name of ACL allow group.
<ADDR_CUSTOM_GROUP_NAME_MIXED>Custom group address object name.
Example: *Sales Group*
- deny**Set MAC filter deny list.
- default**Default SonicPoint ACL deny group.
- group**Name of ACL deny group.
<ADDR_CUSTOM_GROUP_NAME_MIXED>Custom group address object name.
Example: *Sales Group*

Example

access-list allow all deny default

Syntax

```
mic-failure acl-blacklist
```

Mode

Radio N
Radio 2.4GHz

Description

Enable MIC failure ACL blacklist.

Example

```
mic-failure acl-blacklist
```

Syntax

```
no mic-failure acl-blacklist
```

Mode

Radio N
Radio 2.4GHz

Description

Disable MIC failure ACL blacklist.

Example

```
no mic-failure acl-blacklist
```

Syntax

```
mic-failure frequency <UINT8>
```

Mode

Radio N
Radio 2.4GHz

Description

Set MIC failure frequency threshold (times / minute).

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: 123

Example

```
mic-failure frequency 3
```

Syntax

```
virtual-access-point wep-key { { key1 | key2 | key3 | key4 } { { type { 128 | 152 | 64 } value <ENC_PASSWORD> } } | default { 1 | 2 | 3 | 4 } } | method { { alphanumeric | hexadecimal } } }
```

Mode

Radio N
Radio 2.4GHz

Description

Set virtual access point WEP key configuration.

Options

<i>key1</i>	Key 1.
<i>key2</i>	Key 2.
<i>key3</i>	Key 3.
<i>key4</i>	Key 4.
<i>type</i>	Set WEP key type.
<i>128</i>	128 bits.
<i>152</i>	152 bits.
<i>64</i>	64 bits.
<i>value</i>	Set WEP key value.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>
<i>default</i>	Set virtual access point WEP default key.
<i>1</i>	Key 1.
<i>2</i>	Key 2.
<i>3</i>	Key 3.
<i>4</i>	Key 4.
<i>method</i>	Set virtual access point WEP key method.
<i>alphanumeric</i>	Alphanumeric.
<i>hexadecimal</i>	Hexadecimal.

Example

```
virtual-access-point wep-key method alphanumeric
virtual-access-point wep-key default 1
virtual-access-point wep-key 1 type 64 value wepke
```

Syntax

```
no virtual-access-point wep-key { key1 | key2 | key3 | key4 }
```

Mode

Radio N
Radio 2.4GHz

Description

Clear virtual access point WEP key type.

Options

- key1* Key 1.
- key2* Key 2.
- key3* Key 3.
- key4* Key 4.

Example

```
no virtual-access-point wep-key key 1 type
```

Syntax

```
authentication-type { wep { { both | open-system | shared-key } } | wpa { { eap | psk } } | wpa2 { { auto { { eap | psk } } | eap | psk } } | wpa3 { { eap | eap-192b | owe | psk | wpa2-auto { { eap | psk } } } } }
```

Mode

Radio N
Radio 2.4GHz

Description

Set WEP/WPA authentication type.

Options

wep	WEP.
both	WEP - both (open system and shared key).
open-system	WEP - open system.
shared-key	WEP - shared key.
wpa	WPA.
eap	WPA - EAP.
psk	WPA - PSK.
wpa2	WPA2.
auto	WPA2 - AUTO.
eap	WPA2 - AUTO - EAP.
psk	WPA2 - AUTO - PSK.
eap	WPA2 - EAP.
psk	WPA2 - PSK.
wpa3	WPA3.
eap	WPA3 - EAP.
eap-192b	WPA3 - EAP - 192B.
owe	WPA3 - OPEN.
psk	WPA3 - PSK.
wpa2-auto	WPA3/WPA2 - AUTO.
eap	WPA3/WPA2 - EAP.
psk	WPA3/WPA2 - PSK.

Example

```
authentication-type wep both
```

Syntax

`no wep-key { { key1 | key2 | key3 | key4 } value | type }`

Mode

Radio N
Radio 2.4GHz

Description

Clear WEP key type.

Options

- key1** Key 1.
- key2** Key 2.
- key3** Key 3.
- key4** Key 4.
- value** Clear WEP key value.
- type** Clear WEP key type.

Example

`no wep-key type`

Syntax

`wep-key { { key1 | key2 | key3 | key4 } value <ENC_PASSWORD> | default { { 1 | 2 | 3 | 4 } } | method { { alphanumeric | hexadecimal } } | type { { 128 | 152 | 64 | none } } }`

Mode

Radio N
Radio 2.4GHz

Description

Set WEP key configuration.

Options

- key1** Key 1.
- key2** Key 2.
- key3** Key 3.
- key4** Key 4.
- value** Set WEP key value.
- <ENC_PASSWORD>** Password.
Example: `secret`
- default** Set WEP default key.
- 1** Key 1.
- 2** Key 2.
- 3** Key 3.
- 4** Key 4.

<i>method</i>	Set WEP key method.
<i>alphanumeric</i>	Alphanumeric.
<i>hexadecimal</i>	Hexadecimal.
<i>type</i>	Set WEP key type.
<i>128</i>	128 bits.
<i>152</i>	152 bits.
<i>64</i>	64 bits.
<i>none</i>	Clear WEP key type.

Example

```
wep-key method alphaNumeric
wep-key default 1
wep-key type 64
wep-key 1 value wepKeyValue1
```

Syntax

```
wpa auth-balance-method { local-radius-first | local-radius-only | remote-radius-first | remote-radius-only }
```

Mode

Radio N
Radio 2.4GHz

Description

Set authentication balance method.

Options

<i>local-radius-first</i>	Local radius server first.
<i>local-radius-only</i>	Only local radius server.
<i>remote-radius-first</i>	Local radius server as failover mechanism.
<i>remote-radius-only</i>	Only remote radius server.

Example

```
wpa auth-balance-method local-radius-first
```

Syntax

```
wpa cipher-type { aes | auto | gcmp | tkip }
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA cipher type.

Options

<i>aes</i>	AES.

auto Auto.

gcmp AES-GCMP.

tkip TKIP.

Example

```
wpa cipher-type aes
```

Syntax

```
wpa group-key-interval <UINT32>
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA group key interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
wpa group-key-interval 86400
```

Syntax

```
wpa passphrase <ENC_PASSWORD>
```

Mode

Radio N
Radio 2.4GHz

Description

Set WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
wpa passphrase mywpassphrase
```

Syntax

```
no wpa passphrase
```

Mode

Radio N
Radio 2.4GHz

Description

Clear WPA passphrase.

Example

no wpa passphrase

Syntax

wpa pmf [enabled | required]

Mode

Radio N
Radio 2.4GHz

Description

Set WPA PMF(Protected Management Frame) option.

Options

enabled Enable PMF(Protected Management Frame) option.

required Clients must enable the service to connect the AP.

Example

wpa pmf

Syntax

no wpa pmf

Mode

Radio N
Radio 2.4GHz

Description

Disable PMF(Protected Management Frame) option.

Example

no wpa pmf

Syntax

remote-mac-access-control

Mode

Radio N
Radio 2.4GHz

Description

Enable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

remote-mac-access-control

Syntax

no remote-mac-access-control

Mode

Radio N
Radio 2.4GHz

Description

Disable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
no remote-mac-access-control
```

Syntax

```
hide-ssid
```

Mode

Radio N
Radio 2.4GHz

Description

Enable hide SSID in beacon.

Example

```
hide-ssid
```

Syntax

```
no hide-ssid
```

Mode

Radio N
Radio 2.4GHz

Description

Disable hide SSID in beacon.

Example

```
no hide-ssid
```

Syntax

```
ids-scan schedule { days <SCHED_DAYS> time <SCHED_TIME_BEGIN> <SCHED_TIME_END> | name <SCHED_NAME> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set schedule for IDS scan.

Options

days	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
time	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>

<i>name</i>	Schedule object name.
<i><SCHED_NAME></i>	Schedule object name. Example: <i>Work Hours</i>

Example

ids-scan schedule name "Weekend Hours"

Syntax

no ids-scan schedule

Mode

Radio N
Radio 2.4GHz

Description

Disable IDS scan schedule.

Example

no ids-scan schedule

Syntax

data-rate <SONICPOINT_RADIO_DATA_RATE>

Mode

Radio N
Radio 2.4GHz

Description

Set data rate.

Options

<i><SONICPOINT_RADIO_DATA_RATE></i>	SonicPoint radio data rate. Example: <i>best</i>

Example

data-rate best

Syntax

transmit-power { eighth | full | half | minimum | quarter }

Mode

Radio N
Radio 2.4GHz

Description

Set radio transmit power.

Options

<i>eighth</i>	Eighth (-9 dB).
<i>full</i>	Full power.
<i>half</i>	Half (-3 dB).

minimum Minimum.

quarter Quarter (-6 dB).

Example

```
transmit-power half
```

Syntax

```
antenna-diversity best
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio antenna diversity.

Options

best Best.

Example

```
antenna-diversity best
```

Syntax

```
interval { beacon <UINT16> | dtim <UINT8> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio interval.

Options

beacon Set radio beacon interval in milliseconds.
<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

dtim Set radio DTIM interval.
<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
interval beacon 100  
interval dtim 1
```

Syntax

```
threshold { fragmentation <UINT16> | rts <UINT16> }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio threshold in bytes.

Options

<i>fragmentation</i>	Set radio fragmentation threshold in bytes.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>
<i>rts</i>	Set radio RTS threshold in bytes.
<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
threshold fragmentation 2346
threshold rts 2346
```

Syntax

```
max-clients <UINT8>
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio maximum client associations.

Options

<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>

Example

```
max-clients 32
```

Syntax

```
station-inactivity-timeout <UINT16>
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio station inactivity timeout in seconds.

Options

<i><UINT16></i>	Integer in the form: D OR 0xHHHH. Example: <i>123</i>

Example

```
station-inactivity-timeout 300
```

Syntax

```
preamble-length { long | short }
```

Mode

Radio N
Radio 2.4GHz

Description

Set radio preamble length.

Options

long Long.

short Short.

Example

preamble-length long

Syntax

protection mode { always | auto }

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection mode.

Options

always Always.

auto Auto.

Example

protection mode always

Syntax

no protection mode

Mode

Radio N
Radio 2.4GHz

Description

Set no radio protection mode.

Example

no protection mode

Syntax

protection rate { 1 | 11 | 2 | 5 }

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection rate in Mbps.

Options

- 1 Data rate.
- 11 Data rate.
- 2 Data rate.
- 5 Data rate.

Example

protection rate 5

Syntax

protection type { cts-only | rts-cts }

Mode

Radio N
Radio 2.4GHz

Description

Set the radio protection type.

Options

- cts-only CTS-only.
- rts-cts RTS-CTS.

Example

protection type cts-only

Syntax

short-slot-time

Mode

Radio N
Radio 2.4GHz

Description

Enable short slot time.

Example

short-slot-time

Syntax

no short-slot-time

Mode

Radio N
Radio 2.4GHz

Description

Disable short slot time.

Example

```
no short-slot-time
```

Syntax

```
deny-b
```

Mode

Radio N
Radio 2.4GHz

Description

Enable does not allow 802.11b clients to connect.

Example

```
deny-b
```

Syntax

```
no deny-b
```

Mode

Radio N
Radio 2.4GHz

Description

Disable does not allow 802.11b clients to connect.

Example

```
no deny-b
```

Syntax

```
wds-ap
```

Mode

Radio N
Radio 2.4GHz

Description

Enable WDS AP.

Example

```
wds-ap
```

Syntax

```
no wds-ap
```

Mode

Radio N
Radio 2.4GHz

Description

Disable WDS AP.

Example

no wds-ap

Syntax

wmm <WMM_PROFILE>

Mode

Radio N
Radio 2.4GHz

Description

Set WMM (Wi-Fi multimedia).

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

wmm wmmprofile

Syntax

no wmm

Mode

Radio N
Radio 2.4GHz

Description

Disable WMM (Wi-Fi multimedia).

Example

no wmm

Syntax

green-ap enable

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint green AP.

Example

greep-ap enable

Syntax

no green-ap enable

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint green AP.

Example

```
no greep-ap enable
```

Syntax

```
green-ap timeout <UINT16>
```

Mode

Radio N
Radio 2.4GHz

Description

SonicPoint green AP set timeout.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
green-ap timeout 20
```

Syntax

```
rss i enable
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint radio n rssi.

Example

```
rss i enable
```

Syntax

```
no rss i enable
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint rssi.

Example

```
no rss i enable
```

Syntax

```
rss i threshold <INT16>
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint rsii and set threshold.

Options

<***INT16***> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
rss i threshold -95
```

Syntax

```
airtime-fairness
```

Mode

Radio N
Radio 2.4GHz

Description

Enable SonicPoint airtime fairness.

Example

```
airtime-fairness
```

Syntax

```
no airtime-fairness
```

Mode

Radio N
Radio 2.4GHz

Description

Disable SonicPoint airtime fairness.

Example

```
no airtime-fairness
```

Syntax

```
80211r { enable | ft-over-ds | mix-mode }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211r.

Options

<i>enable</i>	Enable IEEE802.11r.
<i>ft-over-ds</i>	Enable IEEE802.11r FT over DS.
<i>mix-mode</i>	Enable IEEE802.11r mix mode.

Example

```
80211r enable
80211r ft-over-ds 80211r mix-mode
```

Syntax

```
no 80211r { enable | ft-over-ds | mix-mode }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211r.

Options

<i>enable</i>	Enable IEEE802.11r.
<i>ft-over-ds</i>	Disable IEEE802.11r FT over DS.
<i>mix-mode</i>	Disable IEEE802.11r mix mode.

Example

```
no 80211r enable
no 80211r ft-over-ds no 80211r mix-mode
```

Syntax

```
80211k neighbour-report
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211k.

Example

```
80211k neighbour-report
```

Syntax

```
no 80211k neighbour-report
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211k.

Example

```
no 80211k neighbour-report
```

Syntax

```
80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Enable IEEE802.11v BSS transition management.

wnm-sleep Enable IEEE802.11v WNM sleep mode.

Example

```
80211v bss-trans-mgmt
```

Syntax

```
no 80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

Radio N
Radio 2.4GHz

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Disable IEEE802.11v BSS transition management.

wnm-sleep Disable IEEE802.11v WNM sleep mode.

Example

```
no 80211v bss-trans-mgmt
```

Syntax

```
ids
```

Mode

SonicPoint

Description

Enter SonicPoint IDS mode.

Example

```
ids
```

Syntax

```
scan sonicpoint <SONICPOINT_IDS_SCAN_NAME> { both | radio { 2400mhz | 5000mhz } }
```

Mode

SonicPoint IDS

Description

Perform SonicPoint scan.

Options

<SONICPOINT_IDS_SCAN_NAME>	SonicPoint IDS scan name. Example: <i>mySonicpointn</i>
both	802.11 both 2.4G and 5G radio.
radio	802.11n 2.4G radio or 5G radio.
2400mhz	802.11n 2.4G radio.
5000mhz	802.11n 5G radio.

Example

```
scan sonicpoint mySP both
scan sonicpoint mySP radio 2400mhz
scan sonicpoint mySP radio 5000mhz
```

Syntax

```
scan all
```

Mode

SonicPoint IDS

Description

Perform SonicPoints scan all.

Example

```
scan all
```

Syntax

```
authorizing-access-point mac <SONICPOINT_DETECTED_AP_MAC>
```

Mode

SonicPoint IDS

Description

Authorizing the access point.

Options

mac	Detected by the SonicPoint.
<SONICPOINT_DETECTED_AP_MAC>	Detected access point MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>

Example

```
authorizing-access-point mac 01:02:03:04:05:06
```

Syntax

widp

Mode

SonicPoint

Description

Enter SonicPoint wireless intrusion detection and prevention mode.

Example

widp

Syntax

enable

Mode

SonicPoint WIDP

Description

Enable SonicPoint WIDP.

Example

enable

Syntax

no enable

Mode

SonicPoint WIDP

Description

Disable SonicPoint WIDP.

Example

no enable

Syntax

authorized-access-point { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }

Mode

SonicPoint WIDP

Description

Set authorized access points.

Options

<i>all</i>	All authorized access points.
<i>group</i>	Specify MAC address object group for authorized access points.

<ADDR_CUSTOM_GROUP_NAME_MIXED> Custom group address object name.
Example: *Sales Group*

Example

```
authorized-access-point all
```

Syntax

```
rogue-access-point { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }
```

Mode

SonicPoint WIDP

Description

Set rogue access points.

Options

all	All rogue access points.
group	Specify MAC address object group for rogue access points.
<ADDR_CUSTOM_GROUP_NAME_MIXED>	Custom group address object name. Example: <i>Sales Group</i>

Example

```
rogue-access-point all
```

Syntax

```
unauthorized-access-point { any | connected }
```

Mode

SonicPoint WIDP

Description

Enable add any unauthorized AP or connected unauthorized AP into rogue AP list.

Options

any	Enable add any unauthorized AP into rogue AP list.
connected	Enable add connected unauthorized AP into rogue AP list.

Example

```
unauthorized-access-point any  
unauthorized-access-point connected
```

Syntax

```
no unauthorized-access-point { any | connected }
```

Mode

SonicPoint WIDP

Description

Disable add any unauthorized AP or connected unauthorized AP into rogue AP list.

Options

- any*** Disable add any unauthorized AP into rogue AP list.
- connected*** Disable add connected unauthorized AP into rogue AP list.

Example

```
no unauthorized-access-point any
no unauthorized-access-point connected
```

Syntax

```
arp-cache-lookup
```

Mode

SonicPoint WIDP

Description

Enable ARP cache lookup to detect connected rogue AP.

Example

```
arp-cache-lookup
```

Syntax

```
no arp-cache-lookup
```

Mode

SonicPoint WIDP

Description

Disable ARP cache lookup to detect connected rogue AP.

Example

```
no arp-cache-lookup
```

Syntax

```
active-probe
```

Mode

SonicPoint WIDP

Description

Enable active probe to detect connected rogue AP.

Example

```
active-probe
```

Syntax

```
no active-probe
```

Mode

SonicPoint WIDP

Description

Disable active probe to detect connected rogue AP.

Example

```
no active-probe
```

Syntax

```
evil-twin
```

Mode

SonicPoint WIDP

Description

Enable add evil twin into rogue AP list.

Example

```
evil-twin
```

Syntax

```
no evil-twin
```

Mode

SonicPoint WIDP

Description

Disable add evil twin into rogue AP list.

Example

```
no evil-twin
```

Syntax

```
block-traffic { all | group <ADDR_CUSTOM_GROUP_NAME_MIXED> }
```

Mode

SonicPoint WIDP

Description

Enable block traffic from rogue AP and its associated clients.

Options

all	All rogue devices.
group	Specify IP address object group for rogue devices.
<ADDR_CUSTOM_GROUP_NAME_MIXED>	Custom group address object name. Example: <i>Sales Group</i>

Example

```
block-traffic all
```

Syntax

```
no block-traffic
```

Mode

SonicPoint WIDP

Description

Disable block traffic from rogue AP and its associated clients.

Example

```
no block-traffic
```

Syntax

```
disassociate rogue
```

Mode

SonicPoint WIDP

Description

Enable disassociate rogue AP and its associated clients.

Example

```
disassociate rogue
```

Syntax

```
no disassociate rogue
```

Mode

SonicPoint WIDP

Description

Disable disassociate rogue AP and its associated clients.

Example

```
no disassociate rogue
```

Syntax

```
disassociate krack
```

Mode

SonicPoint WIDP

Description

Enable disassociate client from KRACK MITM AP.

Example

```
disassociate krack
```

Syntax

```
no disassociate krack
```

Mode

SonicPoint WIDP

Description

Disable disassociate client from KRACK MITM AP.

Example

```
no disassociate krack
```

Syntax

```
rf-monitoring
```

Mode

SonicPoint

Description

Enter SonicPoint RF monitoring configuration mode.

Example

```
rf-monitoring
```

Syntax

```
measurement-interval <UINT16>
```

Mode

RF Monitoring

Description

Set the RF monitoring measurement interval.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

```
measurement-interval 300
```

Syntax

```
management-frame-flood
```

Mode

RF Monitoring

Description

Enable management frame flood threat detection.

Example

```
management-frame-flood
```

Syntax

no management-frame-flood

Mode

RF Monitoring

Description

Disable management frame flood threat detection.

Example

no management-frame-flood

Syntax

null-probe-response

Mode

RF Monitoring

Description

Enable null probe response threat detection.

Example

null-probe-response

Syntax

no null-probe-response

Mode

RF Monitoring

Description

Disable null probe response threat detection.

Example

no null-probe-response

Syntax

broadcasting-deauthentication

Mode

RF Monitoring

Description

Enable broadcasting deauthentication threat detection.

Example

broadcasting-deauthentication

Syntax

no broadcasting-deauthentication

Mode

RF Monitoring

Description

Disable broadcasting deauthentication threat detection.

Example

```
no broadcasting-deauthentication
```

Syntax

```
station-with-invalid-ssid
```

Mode

RF Monitoring

Description

Enable valid station with invalid SSID threat detection.

Example

```
station-with-invalid-ssid
```

Syntax

```
no station-with-invalid-ssid
```

Mode

RF Monitoring

Description

Disable valid station with invalid SSID threat detection.

Example

```
no station-with-invalid-ssid
```

Syntax

```
wellenreiter
```

Mode

RF Monitoring

Description

Enable wellenreiter detection threat detection.

Example

```
wellenreiter
```

Syntax

```
no wellenreiter
```

Mode

RF Monitoring

Description

Disable wellenreiter detection threat detection.

Example

```
no wellenreiter
```

Syntax

```
ad-hoc-station
```

Mode

RF Monitoring

Description

Enable AD-Hoc station threat detection.

Example

```
ad-hoc-station
```

Syntax

```
no ad-hoc-station
```

Mode

RF Monitoring

Description

Disable AD-Hoc station threat detection.

Example

```
no ad-hoc-station
```

Syntax

```
long-duration
```

Mode

RF Monitoring

Description

Enable long duration threat detection.

Example

```
long-duration
```

Syntax

```
no long-duration
```

Mode

RF Monitoring

Description

Disable long duration threat detection.

Example

no long-duration

Syntax

unassociated-station

Mode

RF Monitoring

Description

Enable unassociated station threat detection.

Example

unassociated-station

Syntax

no unassociated-station

Mode

RF Monitoring

Description

Disable unassociated station threat detection.

Example

no unassociated-station

Syntax

netstumbler

Mode

RF Monitoring

Description

Enable netstumbler threat detection.

Example

netstumbler

Syntax

no netstumbler

Mode

RF Monitoring

Description

Disable netstumbler threat detection.

Example

no netstumbler

Syntax

eapol-packet-flood

Mode

RF Monitoring

Description

Enable EAPOL packet flood threat detection.

Example

eapol-packet-flood

Syntax

no eapol-packet-flood

Mode

RF Monitoring

Description

Disable EAPOL packet flood threat detection.

Example

no eapol-packet-flood

Syntax

weak-wep-iv

Mode

RF Monitoring

Description

Enable weak WEP IV threat detection.

Example

weak-wep-iv

Syntax

no weak-wep-iv

Mode

RF Monitoring

Description

Disable weak WEP IV threat detection.

Example

no weak-wep-iv

Syntax

watch station <RFM_DETECTED_STATION_MAC>

Mode

RF Monitoring

Description

Add station into watch list.

Options

<RFM_DETECTED_STATION_MAC> Rf monitoring detected station MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
watch station 01:02:03:04:05:06
```

Syntax

```
no watch station <RFM_DETECTED_STATION_MAC>
```

Mode

RF Monitoring

Description

Remove station from watch list.

Options

<RFM_DETECTED_STATION_MAC> Rf monitoring detected station MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH.
Example: *00:0C:F1:56:98:AD*

Example

```
no watch station 01:02:03:04:05:06
```

Syntax

```
clear rf-monitoring statistics
```

Mode

RF Monitoring

Description

Clear RF monitoring statistics information.

Example

```
clear rf-monitoring statistics
```

Syntax

```
fairnet enable
```

Mode

SonicPoint

Description

Enable FairNet.

Example

```
fairnet enable
```

Syntax

no fairnet enable

Mode

SonicPoint

Description

Disable FairNet.

Example

no fairnet enable

Syntax

fairnet policy direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE> [rate min <UINT32> max <UINT32>]

Mode

SonicPoint

Description

Add/edit FairNet policy and enter its configuration mode.

Options

<i>direction</i>	Specify direction.
<i>both</i>	Both.
<i>downlink</i>	Downlink (AP to client).
<i>uplink</i>	Uplink (client to AP).
<i>range</i>	Specify IP range.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>interface</i>	Specify interface.
<i><FAIRNET_INTERFACE></i>	Fairnet interface name. Example: <i>X0</i>
<i>rate</i>	Specify rate of FairNet policy in kbps.
<i>min</i>	Specify min rate of FairNet policy in kbps.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>
<i>max</i>	Specify maximum rate of FairNet policy in kbps.
<i><UINT32></i>	Integer in the form: D OR 0xHHHHHHHH. Example: <i>123</i>

Example

fairnet policy direction both range 192.168.168.100 192.168.168.200 interface X2

Syntax

no fairnet policy direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE>

Mode

SonicPoint

Description

Delete FairNet policy.

Options

<i>direction</i>	Specify direction.
<i>both</i>	Both.
<i>downlink</i>	Downlink (AP to client).
<i>uplink</i>	Uplink (client to AP).
<i>range</i>	Specify IP range.
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i><IPV4_HOST></i>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>interface</i>	Specify interface.
<i><FAIRNET_INTERFACE></i>	Fairnet interface name. Example: <i>X0</i>

Example

no fairnet policy direction both range 192.168.168.100 192.168.168.200 interface X2

Syntax

no fairnet policies

Mode

SonicPoint

Description

Delete all FairNet policies.

Example

no fairnet policies

Syntax

enable

Mode

FairNet Policy

Description

Enable this FairNet policy.

Example

enable

Syntax

no enable

Mode

FairNet Policy

Description

Disable this FairNet policy.

Example

```
no enable
```

Syntax

```
direction { both | downlink | uplink }
```

Mode

FairNet Policy

Description

Set direction of FairNet policy.

Options

both Both.

downlink Downlink (AP to client).

uplink Uplink (client to AP).

Example

```
direction both
```

Syntax

```
range <IPV4_HOST> <IPV4_HOST>
```

Mode

FairNet Policy

Description

Set IP range of FairNet policy.

Options

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

<IPV4_HOST> IPv4 Address in the form: a.b.c.d.
Example: *192.168.168.168*

Example

```
range 192.168.168.100 192.168.168.200
```

Syntax

```
interface <FAIRNET_INTERFACE>
```

Mode

FairNet Policy

Description

Set interface of FairNet policy.

Options

<FAIRNET_INTERFACE> Fairnet interface name.
Example: *X0*

Example

```
interface X2
```

Syntax

```
rate min <UINT32> max <UINT32>
```

Mode

FairNet Policy

Description

Set rate of FairNet policy in kbps.

Options

- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*
- max** Specify maximum rate of FairNet policy in kbps.
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
rate min 1000 max 2000
```

Syntax

```
rrm
```

Mode

SonicPoint

Description

Enter SonicPoint RRM configuration mode.

Example

```
rrm
```

Syntax

```
enable
```

Mode

Radio Resource Management

Description

Enable rrm.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Description

Disable rrm.

Example

```
no enable
```

Syntax

```
sta threshold <UINT32>
```

Mode

Radio Resource Management

Description

Set threshold for bad STA quality.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
sta threshold 20
```

Syntax

```
radio threshold <UINT32>
```

Mode

Radio Resource Management

Description

Set threshold for bad RADIO quality.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
radio threshold 20
```

Syntax

```
dcs { global | local }
```

Mode

Radio Resource Management

Description

Set dcs mode.

Options

global Set dcs mode as global dcs.

local Set dcs mode as local dcs.

Example

```
dcs global
```

Syntax

```
dcsscheme24g { safe | steady | swift }
```

Mode

Radio Resource Management

Description

Set 2.4G dcs scheme.

Options

safe Set 2.4G dcs scheme safe mode.

steady Set 2.4G dcs scheme steady mode.

swift Set 2.4G dcs scheme swift mode.

Example

```
dcsscheme24g safe
```

Syntax

```
dcsscheme5g { safe | steady | swift }
```

Mode

Radio Resource Management

Description

Set 5G dcs scheme.

Options

safe Set 5G dcs scheme safe mode.

steady Set 5G dcs scheme steady mode.

swift Set 5G dcs scheme swift mode.

Example

```
dcsscheme5g safe
```

Syntax

```
force-switch { 24g | 5g }
```

Mode

Radio Resource Management

Description

Force to Switch 2.4G/5G channel to a better one.

Options

24g Force switch 2.4g radio channel

5g Force switch 5g radio channel

Example

```
force-switch 5g
```

Syntax

```
wmm profile <WMM_PROFILE>
```

Mode

SonicPoint

Description

Add/edit WiFi multimedia profile and enter its configuration mode.

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

```
wmm profile corpwifiwmm
```

Syntax

```
no wmm profile <WMM_PROFILE>
```

Mode

SonicPoint

Description

Delete the specified WiFi multimedia profile.

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

```
no wmm profile corpwifiwmm
```

Syntax

```
no wmm profiles
```

Mode

SonicPoint

Description

Delete all WiFi multimedia profiles.

Example

```
no wmm profiles
```

Syntax

name <WMM_PROFILE>

Mode

WiFi Multimedia Profile

Description

Set the WiFi multimedia profile name.

Options

<WMM_PROFILE> WiFi multimedia profile name.
Example: *abc*

Example

name corpwifiwmm

Syntax

no access-point { *ac-be* | *ac-bk* | *ac-vi* | *ac-vo* } { [*cwmin*] [*cwmax*] }

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for access point category.

Options

ac-be Set the WMM parameters for access point category AC_BE (0).

ac-bk Set the WMM parameters for access point category AC_BK (1).

ac-vi Set the WMM parameters for access point category AC_VI (2).

ac-vo Set the WMM parameters for access point category AC_VO (3).

cwmin Clear the CW min value.

cwmax Clear the CW max value.

Example

no access-point ac-be cwmin cwmax
no access-point ac-be cwmin
no access-point ac-be cwmax

Syntax

access-point { *ac-be* | *ac-bk* | *ac-vi* | *ac-vo* } { [*cwmin* <UINT8>] [*cwmax* <UINT8>] [*aifs* <UINT8>] }

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for access point category.

Options

ac-be Set the WMM parameters for access point category AC_BE (0).

- ac-bk** Set the WMM parameters for access point category AC_BK (1).
- ac-vi** Set the WMM parameters for access point category AC_VI (2).
- ac-vo** Set the WMM parameters for access point category AC_VO (3).
- cwmin** Set the CW min value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- cwmax** Set the CW max value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- aifs** Set the AIFS value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

Example

```
access-point ac-be cwmin 4 cwmax 6 aifs 3
access-point ac-be cwmin 4 cwmax 6
access-point ac-be cwmin 4
access-point ac-be cwmax 6
access-point ac-be aifs 3
```

Syntax

```
no station { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmin ] [ cwmax ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for station category.

Options

- ac-be** Set the WMM parameters for station category AC_BE (0).
- ac-bk** Set the WMM parameters for station category AC_BK (1).
- ac-vi** Set the WMM parameters for station category AC_VI (2).
- ac-vo** Set the WMM parameters for station category AC_VO (3).
- cwmin** Clear the CW min value.
- cwmax** Clear the CW max value.

Example

```
no station ac-be cwmin cwmax
no station ac-be cwmin
no station ac-be cwmax
```

Syntax

```
station { ac-be | ac-bk | ac-vi | ac-vo } { [ cwmin <UINT8> ] [ cwmax <UINT8> ] [ aifs <UINT8> ] }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM parameter for station category.

Options

- ac-be** Set the WMM parameters for station category AC_BE (0).
- ac-bk** Set the WMM parameters for station category AC_BK (1).
- ac-vi** Set the WMM parameters for station category AC_VI (2).
- ac-vo** Set the WMM parameters for station category AC_VO (3).
- cwmin** Set the CW min value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- cwmax** Set the CW max value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- aifs** Set the AIFS value.
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

Example

```
station ac-be cwmin 4 cwmax 10 aifs 3
station ac-be cwmin 4 cwmax 10
station ac-be cwmin 4
station ac-be cwmax 10
station ac-be aifs 3
```

Syntax

```
no mapping { ac-be | ac-bk | ac-vi | ac-vo }
```

Mode

WiFi Multimedia Profile

Description

Clear the WMM DSCP mapping.

Options

- ac-be** Clear the WMM DSCP mapping for category AC_BE (0).
- ac-bk** Clear the WMM DSCP mapping for category AC_BK (1).
- ac-vi** Clear the WMM DSCP mapping for category AC_VI (2).
- ac-vo** Clear the WMM DSCP mapping for category AC_VO (3).

Example

```
no mapping ac-bk
```

Syntax

```
mapping { ac-be <UINT8> | ac-bk <UINT8> | ac-vi <UINT8> | ac-vo <UINT8> }
```

Mode

WiFi Multimedia Profile

Description

Set the WMM DSCP mapping.

Options

- ac-be** Set the WMM DSCP mapping for category AC_BE (0).
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

- ac-bk** Set the WMM DSCP mapping for category AC_BK (1).
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- ac-vi** Set the WMM DSCP mapping for category AC_VI (2).
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123
- ac-vo** Set the WMM DSCP mapping for category AC_VO (3).
- <UINT8>** Integer in the form: D OR 0xHH.
Example: 123

Example

```
mapping ac-bk 8
```

Syntax

```
floor-plan <SONICPOINT_FLOOR_PLAN_NAME>
```

Mode

SonicPoint

Description

Add/edit access point floor plan.

Options

- <SONICPOINT_FLOOR_PLAN_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
floor-plan "Corp main floor wifi"
```

Syntax

```
no floor-plan <SONICPOINT_FLOOR_PLAN_NAME>
```

Mode

SonicPoint

Description

Delete access point floor plan.

Options

- <SONICPOINT_FLOOR_PLAN_NAME>** Word in the form: WORD or \"QUOTED STRING\".
Example: abc

Example

```
no floor-plan "Corp main floor wifi"
```

Syntax

```
no floor-plans
```

Mode

SonicPoint

Description

Delete all access point floor plans.

Example

```
no floor-plans
```

Syntax

```
name <SONICPOINT_FLOOR_PLAN_NAME>
```

Mode

Access Point Floor Plan

Description

Set access point floor plan name.

Options

<SONICPOINT_FLOOR_PLAN_NAME> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
floor-plan "Corp main floor wifi"
```

Syntax

```
comment <WORD>
```

Mode

Access Point Floor Plan

Description

Set access point floor plan comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
comment "Location of access points on main floor"
```

Syntax

```
no comment
```

Mode

Access Point Floor Plan

Description

Clear access point floor plan comment.

Example

```
no comment
```

Syntax

image <WORD>

Mode

Access Point Floor Plan

Description

Set access point floor plan comment.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

image "HHHHHHHHHH"

Syntax

no image

Mode

Access Point Floor Plan

Description

Clear access point floor plan image.

Example

no image

Syntax

image-width <UINT32>

Mode

Access Point Floor Plan

Description

Set access point floor plan image width.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

image-width 800

Syntax

no image-width

Mode

Access Point Floor Plan

Description

Clear access point floor plan image width.

Example

no image-width

Syntax

image-height <UINT32>

Mode

Access Point Floor Plan

Description

Set access point floor plan image height.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: 123

Example

image-height 400

Syntax

no image-height

Mode

Access Point Floor Plan

Description

Clear access point floor plan image height.

Example

no image-height

Syntax

scale <DECIMAL>

Mode

Access Point Floor Plan

Description

Set access point floor plan scale.

Options

<DECIMAL> Decimal in the form: n+.n+.
Example: 0.999

Example

scale 10.5

Syntax

no scale

Mode

Description

Clear access point floor plan scale.

Example

no scale

Syntax

export floor-plan <SONICPOINT_FLOOR_PLAN_NAME> { *jpg* | *png* } { *api* | *ftp* <FTP_URL> | *scp* <SCP_URL> [*port* <IPV4_PORT>] }

Mode

Top Level
Config
SonicPoint

Description

Export floor plan image.

Options

<SONICPOINT_FLOOR_PLAN_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>jpg</i>	Export floor plan image as jpg
<i>png</i>	Export floor plan image as png.
<i>api</i>	Export using the api protocol.
<i>ftp</i> <FTP_URL>	Export using the FTP protocol. FTP URL in the form: ftp://username:password@hostname/ Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\/', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\\nftp://username@hostname/\\nftp://hostname/</i>
<i>scp</i> <SCP_URL>	Export using the SCP protocol. SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>
<i>port</i> <IPV4_PORT>	SCP server port Integer in the form: D OR 0xHHHH. Example: <i>80</i>

Example

export floor-plan name jpg ftp ftp://user:password@servername/corpMainFloor.jpg
export floor-plan name png scp user@server:/home/user/corpSecondFloor.png

Syntax

import floor-plan <SONICPOINT_FLOOR_PLAN_NAME> { *api* | *ftp* <FTP_URL> | *scp* <SCP_URL> }

Mode

SonicPoint

Description

Import floor plan image.

Options

<SONICPOINT_FLOOR_PLAN_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
<i>api</i>	Import using the api protocol.
<i>ftp</i>	Import using the FTP protocol.

<FTP_URL>	FTP URL in the form: ftp://username:password@hostname/\n Escape character: ':' -> '\\:', '@' -> '\\\\@', '/' -> '\\\\V', '\\' -> '\\\\\\\\'. Example: <i>ftp://username:password@hostname/\nftp://username@hostname/\nftp://hostname/</i>
scp	Import using the SCP protocol.
<SCP_URL>	SCP URL in the form: userName@serverip:/fileDirectory. Example: <i>userTest@10.10.10.10:/home/userTest/</i>

Example

```
import floor-plan ftp://user:password@servername/corpMainFloor.jpg
import floor-plan name scp user@server:/home/user/corpSecondFloor.png
```

Syntax

```
access-point <SONICPOINT_N_NAME> <UINT32> <UINT32>
```

Mode

Access Point Floor Plan

Description

Add access point to floor plan.

Options

- <SONICPOINT_N_NAME>** SonicPointN name.
Example: *mySonicpointn*
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
access-point c0:ea:e4:58:98:ff 116 24
```

Syntax

```
no access-point <SONICPOINT_N_NAME> <UINT32> <UINT32>
```

Mode

Access Point Floor Plan

Description

Delete access point from floor plan.

Options

- <SONICPOINT_N_NAME>** SonicPointN name.
Example: *mySonicpointn*
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*
- <UINT32>** Integer in the form: D OR 0xHHHHHHHHH.
Example: *123*

Example

```
no access-point c0:ea:e4:58:98:ff 116 24
```

Syntax

```
no access-points
```

Mode

Access Point Floor Plan

Description

Delete all access points from floor plan.

Example

```
no access-points
```

Syntax

```
virtual-access-point group <WIRELESS_VAP_GROUP_NAME>
```

Mode

Wireless

Description

Add/edit virtual access point group and enter its configuration mode.

Options

<WIRELESS_VAP_GROUP_NAME> Wireless VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
virtual-access-point group CorpVAP
```

Syntax

```
virtual-access-point profile <WIRELESS_VAP_PROFILE_NAME>
```

Mode

Wireless

Description

Add/edit virtual access point profile and enter its configuration mode.

Options

<WIRELESS_VAP_PROFILE_NAME> Wireless VAP profile name in the form: WORD or \"QUOTED STRING\".
Example: *vapProfile*

Example

```
virtual-access-point profile CorpVAP
```

Syntax

```
virtual-access-point object <WIRELESS_VAP_NAME>
```

Mode

Wireless

Description

Add/edit virtual access point object and enter its configuration mode.

Options

<WIRELESS_VAP_NAME> Wireless VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

virtual-access-point object CorpVAP

Syntax

no virtual-access-point { object <WIRELESS_VAP_NAME> | objects | profile <WIRELESS_VAP_PROFILE_NAME> | profiles }

Mode

Wireless

Description

Delete the specified virtual access point object, profile or group.

Options

<i>object</i> <i><WIRELESS_VAP_NAME></i>	Delete virtual access point object and enter its configuration mode. Wireless VAP NAME in the form: WORD or \"QUOTED STRING\". Example: <i>vapObject</i>
<i>objects</i>	Delete all virtual access point objects.
<i>profile</i> <i><WIRELESS_VAP_PROFILE_NAME></i>	Delete virtual access point profile and enter its configuration mode. Wireless VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i>
<i>profiles</i>	Delete all virtual access point profiles.

Example

no virtual-access-point object CorpVAP
no virtual-access-point profiles

Syntax

name <VAP_EDIT_NAME>

Mode

Wireless Virtual Access Point Group

Description

Set virtual access point group name.

Options

<i><VAP_EDIT_NAME></i>	VAP object or profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapName</i>

Example

name CorpVAPGroup

Syntax

virtual-access-point <WIRELESS_VAP_NAME>

Mode

Wireless Virtual Access Point Group

Description

Add virtual access point object to this group.

Options

<WIRELESS_VAP_NAME> Wireless VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
virtual-access-point CorpVAPSSID
```

Syntax

```
no virtual-access-point <WIRELESS_VAP_NAME>
```

Mode

Wireless Virtual Access Point Group

Description

Remove virtual access point object from this group.

Options

<WIRELESS_VAP_NAME> Wireless VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
no virtual-access-point CorpVAPSSID
```

Syntax

```
no virtual-access-points
```

Mode

Wireless Virtual Access Point Group

Description

Remove all virtual access point objects from this group.

Example

```
no virtual-access-points
```

Syntax

```
virtual-access-point group <VAP_GROUP>
```

Mode

SonicPoint

Description

Add/edit virtual access point group and enter its configuration mode.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
virtual-access-point group CorpVAP
```

Syntax

virtual-access-point profile <VAP_PROFILE>

Mode

SonicPoint

Description

Add/edit virtual access point profile and enter its configuration mode.

Options

<VAP_PROFILE> VAP profile name in the form: WORD or \"QUOTED STRING\".
Example: *vapProfile*

Example

virtual-access-point profile CorpVAP

Syntax

virtual-access-point object <VAP_NAME>

Mode

SonicPoint

Description

Add/edit virtual access point object and enter its configuration mode.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

virtual-access-point object CorpVAP

Syntax

no virtual-access-point { group <VAP_GROUP> | groups | object <VAP_NAME> | objects | profile <VAP_PROFILE> | profiles }

Mode

SonicPoint

Description

Delete the specified virtual access point object, profile or group.

Options

group Delete virtual access point group and enter its configuration mode.
<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

groups Delete all virtual access point groups.

object Delete virtual access point object and enter its configuration mode.
<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

objects Delete all virtual access point objects.

profile Delete virtual access point profile and enter its configuration mode.
<VAP_PROFILE> VAP profile name in the form: WORD or \"QUOTED STRING\".
Example: *vapProfile*

profiles Delete all virtual access point profiles.

Example

```
no virtual-access-point object CorpVAP
no virtual-access-point groups
```

Syntax

```
name <VAP_GROUP>
```

Mode

SonicPoint Virtual Access Point Group

Description

Set virtual access point group name.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
name CorpVAPGroup
```

Syntax

```
virtual-access-point <VAP_NAME>
```

Mode

SonicPoint Virtual Access Point Group

Description

Add virtual access point object to this group.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

```
virtual-access-point CorpVAPSSID
```

Syntax

```
group <VAP_GROUP>
```

Mode

SonicPoint Virtual Access Point Group

Description

Add virtual access point group to this group.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

```
group CorpVAPGroup
```

Syntax

no virtual-access-point <VAP_NAME>

Mode

SonicPoint Virtual Access Point Group

Description

Remove the specified virtual access point from this group.

Options

<VAP_NAME> VAP NAME in the form: WORD or \"QUOTED STRING\".
Example: *vapObject*

Example

no virtual-access-point CorpVAPSSid

Syntax

no group <VAP_GROUP>

Mode

SonicPoint Virtual Access Point Group

Description

Remove the specified virtual access point group from this group.

Options

<VAP_GROUP> VAP group name in the form: WORD or \"QUOTED STRING\".
Example: *vapGroup*

Example

no group CorpVAPGroup

Syntax

no virtual-access-points

Mode

SonicPoint Virtual Access Point Group

Description

Remove all virtual access point objects from this group.

Example

no virtual-access-points

Syntax

no groups

Mode

SonicPoint Virtual Access Point Group

Description

Remove all virtual access point groups from this group.

Example

no groups

Syntax

name <VAP_EDIT_NAME>

Mode

VAP Profile
Virtual Access Point

Description

Set virtual access point object or profile name.

Options

<VAP_EDIT_NAME> VAP object or profile name in the form: WORD or \"QUOTED STRING\".
Example: *vapName*

Example

name CorpVAP

Syntax

schedule { *always-on* | *days* <SCHED_DAYS> *time* <SCHED_TIME_BEGIN> <SCHED_TIME_END> | *name* <SCHED_NAME> }

Mode

VAP Profile
Virtual Access Point

Description

Set the schedule.

Options

<i>always-on</i>	Always on.
<i>days</i>	Schedule object days.
<SCHED_DAYS>	Days of the week in the form: SU-M-T-W-TH-F-SA. Example: <i>SU-M-TH-SA</i>
<i>time</i>	Schedule object beginning/ending time.
<SCHED_TIME_BEGIN>	Time in the form: DD:DD. Example: <i>12:00</i>
<SCHED_TIME_END>	Time in the form: DD:DD. Example: <i>12:00</i>
<i>name</i>	Schedule object name.
<SCHED_NAME>	Schedule object name. Example: <i>Work Hours</i>

Example

schedule name "Work Hours"

Syntax


```
access-list [ [ allow { { all | default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> } } | deny { { default | group <ADDR_CUSTOM_GROUP_NAME_MIXED> } } | mac-filter-list | use-global-access-list ] ]
```

Mode

VAP Profile
Virtual Access Point

Description

Enable/configure MAC filter list for this VAP.

Options

allow	Set MAC filter allow list.
all	All MAC addresses.
default	Default ACL allow group.
group <ADDR_CUSTOM_GROUP_NAME_MIXED>	Name of ACL allow group. Custom group address object name. Example: <i>Sales Group</i>
deny	Set MAC filter deny list.
default	Default ACL deny group.
group <ADDR_CUSTOM_GROUP_NAME_MIXED>	Name of ACL deny group. Custom group address object name. Example: <i>Sales Group</i>
mac-filter-list	Enable MAC filter list.
use-global-access-list	Enable this VAP to use global ACL settings.

Example

```
access-list allow all deny default
access-list allow default
access-list deny group wirelessAclDenyList
```

Syntax

```
no access-list [ deny | mac-filter-list | use-global-access-list ]
```

Mode

VAP Profile
Virtual Access Point

Description

Disable MAC filter list to use global ACL settings for this VAP.

Options

deny	Disable MAC filter deny list.
mac-filter-list	Disable MAC filter list.
use-global-access-list	Disable this VAP to use global ACL settings.

Example

```
no access-list
no access-list deny
no access-list use-global-access-list
```

Syntax

```
radio-type { sonicpoint | wireless }
```

Mode

VAP Profile

Description

Set virtual access point profile radio type.

Options

sonicpoint Sonicpoint.

wireless Wireless.

Example

```
radio-type sonicpoint
```

Syntax

```
max-clients <UINT8>
```

Mode

VAP Profile

Virtual Access Point

Description

Set maximum client associations.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

```
max-clients 16
```

Syntax

```
wep-key default { 1 | 2 | 3 | 4 }
```

Mode

VAP Profile

Virtual Access Point

Description

Set WEP encryption default key index.

Options

default Set WEP encryption default key index.

1 Key 1.

2 Key 2.

3 Key 3.

4 Key 4.

Example

```
wep-key default 1
```

Syntax

```
authentication-type { wep { { both | open-system | shared-key } } | wpa { { eap | psk } } | wpa2 { { auto { { eap | psk } } | eap | psk } } | wpa3 { { eap | eap-192b | owe | psk | wpa2-auto { { eap | psk } } } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Set WEP/WPA authentication type.

Options

wep	WEP.
both	WEP - both (open system and shared key).
open-system	WEP - open system.
shared-key	WEP - shared key.
wpa	WPA.
eap	WPA - EAP.
psk	WPA - PSK.
wpa2	WPA2.
auto	WPA2 - AUTO.
eap	WPA2 - AUTO - EAP.
psk	WPA2 - AUTO - PSK.
eap	WPA2 - EAP.
psk	WPA2 - PSK.
wpa3	WPA3.
eap	WPA3 - EAP.
eap-192b	WPA3 - EAP - 192B.
owe	WPA3 - OWE.
psk	WPA3 - PSK.
wpa2-auto	WPA3/WPA2 - AUTO.
eap	WPA3/WPA2 - EAP.
psk	WPA3/WPA2 - PSK.

Example

```
authentication-type wep both
```

Syntax

```
wpa auth-balance-method { local-radius-first | local-radius-only | remote-radius-first | remote-radius-only }
```

Mode

VAP Profile
Virtual Access Point

Description

Set authentication balance method.

Options

<i>local-radius-first</i>	Local radius server first.
<i>local-radius-only</i>	Only local radius server.
<i>remote-radius-first</i>	Local radius server as failover mechanism.
<i>remote-radius-only</i>	Only remote radius server.

Example

```
wpa auth-balance-method local-radius-first
```

Syntax

```
cipher-type { aes | auto | gcmp | tkip | wep }
```

Mode

VAP Profile
Virtual Access Point

Description

Set cipher type.

Options

<i>aes</i>	AES.
<i>auto</i>	Auto.
<i>gcmp</i>	AES-GCMP.
<i>tkip</i>	TKIP.
<i>wep</i>	WEP.

Example

```
cipher-type aes
```

Syntax

```
no cipher-type
```

Mode

VAP Profile
Virtual Access Point

Description

Set no cipher.

Example

```
no cipher-type
```

Syntax

```
wpa passphrase <ENC_PASSWORD>
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA passphrase.

Options

<ENC_PASSWORD> Password.
Example: *secret*

Example

```
wpa passphrase mywapassphrase
```

Syntax

```
no wpa passphrase
```

Mode

VAP Profile
Virtual Access Point

Description

Clear WPA passphrase.

Example

```
no wpa passphrase
```

Syntax

```
wpa group-key-interval <UINT32>
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA group key interval in seconds.

Options

<UINT32> Integer in the form: D OR 0xHHHHHHHH.
Example: *123*

Example

```
wpa group-key-interval 86400
```

Syntax

```
wpa pmf [ enabled | required ]
```

Mode

VAP Profile
Virtual Access Point

Description

Set WPA PMF(Protected Management Frame) option.

Options

enabled Enable PMF(Protected Management Frame) option.

required Clients must enable the service to connect the AP.

Example

```
wpa pmf
```

Syntax

```
no wpa pmf
```

Mode

VAP Profile
Virtual Access Point

Description

Disable PMF(Protected Management Frame) option.

Example

```
no wpa pmf
```

Syntax

```
radius { accounting { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } | nas { {  
  identifier { sonicpoint-mac-address | sonicpoint-name | sonicpoint-ssid } | ip <IPV4_HOST> } } | retries <UINT8> | retry-  
  interval <UINT8> | server { server1 | server2 } { { ip <IPV4_HOST> | port <IPV4_PORT> | secret <ENC_PASSWORD> } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Set radius server for virtual access point.

Options

accounting Set radius accounting server.

server1 Radius accounting server 1.

server2 Radius accounting server 2.

ip
<IPV4_HOST> Radius accounting server IP.
IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

port
<IPV4_PORT> Radius accounting server port.
Integer in the form: D OR 0xHHHH.
Example: 80

<i>secret</i>	Radius accounting server secret.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>
<i>nas</i>	Nas settings to radius server.
<i>identifier</i>	Nas identifier to radius server.
<i>sonicpoint-mac-address</i>	SonicPoint's MAC address.
<i>sonicpoint-name</i>	SonicPoint's name.
<i>sonicpoint-ssid</i>	SonicPoint's SSID.
<i>ip</i>	Nas IP to radius server.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>retries</i>	Set radius server retries.
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>retry-interval</i>	Set radius server retry interval (seconds).
<i><UINT8></i>	Integer in the form: D OR 0xHH. Example: <i>123</i>
<i>server</i>	Set radius server.
<i>server1</i>	Radius server 1.
<i>server2</i>	Radius server 2.
<i>ip</i>	Radius server IP.
<i><IPV4_HOST></i>	IPV4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<i>port</i>	Radius server port.
<i><IPV4_PORT></i>	Integer in the form: D OR 0xHHHH. Example: <i>80</i>
<i>secret</i>	Radius server secret.
<i><ENC_PASSWORD></i>	Password. Example: <i>secret</i>

Example

```
radius retries 1
radius retry-interval 20
radius server server1 ip 192.168.168.1
radius server server1 port 1812
radius server server1 secret radsecret
radius server server2 ip 192.168.168.2
radius server server2 port 1812
radius server server2 secret radsecret2
```

.....

Syntax

```
no radius { accouting { server1 | server2 } { { ip | port | secret } } | nas { identifier | ip } | retries | retry-interval |
server { server1 | server2 } { { ip | port | secret } } }
```

Mode

VAP Profile
Virtual Access Point

Description

Clear radius server settings for virtual access point.

Options

<i>accounting</i>	Clear radius accounting server settings.
<i>server1</i>	Clear radius accounting server 1 settings.
<i>server2</i>	Clear radius accounting server 2 settings.
<i>ip</i>	Clear radius accounting server IP.
<i>port</i>	Clear radius accounting server port.
<i>secret</i>	Clear radius accounting server secret.
<i>nas</i>	Clear nas settings to radius server.
<i>identifier</i>	Nas identifier to radius server not included.
<i>ip</i>	Clear nas IP to radius server.
<i>retries</i>	Clear radius server retries.
<i>retry-interval</i>	Clear radius server retry interval.
<i>server</i>	Clear radius server setting.
<i>server1</i>	Clear radius server 1 settings.
<i>server2</i>	Clear radius server 2 settings.
<i>ip</i>	Clear radius server IP.
<i>port</i>	Clear radius server port.
<i>secret</i>	Clear radius server secre.

Example

```
no radius retries
no radius retry-interval
no server server1 ip
no server server1 port
no server server1 secret
no server server2 ip
no server server2 port
no server server2 secret
```

Syntax

```
remote-mac-access-control
```

Mode

VAP Profile
Virtual Access Point

Description

Enable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
remote-mac-access-control
```

Syntax

```
no remote-mac-access-control
```

Mode

VAP Profile
Virtual Access Point

Description

Disable enforce radio wireless access control based on MAC-based authentication policy in remote radius server.

Example

```
no remote-mac-access-control
```

Syntax

```
wds
```

Mode

VAP Profile
Virtual Access Point

Description

Enable virtual access point wireless distribution system.

Example

```
wds
```

Syntax

```
no wds
```

Mode

VAP Profile
Virtual Access Point

Description

Disable virtual access point wireless distribution system.

Example

```
no wds
```

Syntax

```
allow-b
```

Mode

VAP Profile
Virtual Access Point

Description

Allow 802.11b clients to connect.

Example

```
allow-b
```

Syntax

```
no allow-b
```

Mode

Description

Don't allow 802.11b clients to connect.

Example

```
no allow-b
```

Syntax

```
radio-type { sonicpoint | wireless }
```

Mode

Virtual Access Point

Description

Set virtual access point radio type.

Options

sonicpoint Sonicpoint.

wireless Wireless.

Example

```
radio-type sonicpoint
```

Syntax

```
ssid <WORD>
```

Mode

Virtual Access Point

Description

Set virtual access point SSID.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
ssid CorpSSID
```

Syntax

```
no ssid
```

Mode

Virtual Access Point

Description

Clear virtual access point SSID.

Example

no ssid

Syntax

no vlan-id

Mode

Virtual Access Point

Description

Clear virtual access point vlan id.

Example

no vlan-id

Syntax

vlan-id <VAP_VLAN_ID>

Mode

Virtual Access Point

Description

Set virtual access point vlan id.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

vlan-id 100

Syntax

suppress-ssid

Mode

Virtual Access Point

Description

Enable suppress SSID.

Example

suppress-ssid

Syntax

no suppress-ssid

Mode

Virtual Access Point

Description

Disable suppress SSID.

Example

```
no suppress-ssid
```

Syntax

```
enable
```

Mode

Virtual Access Point

Description

Enable virtual access point.

Example

```
enable
```

Syntax

```
no enable
```

Mode

Virtual Access Point

Description

Disable virtual access point.

Example

```
no enable
```

Syntax

```
dynamic-vlan
```

Mode

Virtual Access Point

Description

Enable VAP dynamic vlan assignment id.

Example

```
dynamic-vlan
```

Syntax

```
no dynamic-vlan
```

Mode

Virtual Access Point

Description

Disable VAP dynamic vlan assignment id.

Example

```
no dynamic-vlan
```

Syntax

vlan <VAP_VLAN_ID>

Mode

Virtual Access Point

Description

Set SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

vlan 4

Syntax

no vlan <VAP_VLAN_ID>

Mode

Virtual Access Point

Description

Clear SonicPoint dynamic VLAN ID.

Options

<VAP_VLAN_ID> VLAN ID.
Example: 100

Example

no vlan 4

Syntax

no vlans

Mode

Virtual Access Point

Description

Clear SonicPoint dynamic VLAN IDs.

Example

no vlans

Syntax

profile { *sonicpoint* <VAP_PROFILE> | *wireless* <WIRELESS_VAP_PROFILE_NAME> }

Mode

Virtual Access Point

Description

Set virtual access point profile used.

Options

<i>sonicpoint</i>	Specify profile name.
<VAP_PROFILE>	VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i>
<i>wireless</i>	Specify profile name.
<WIRELESS_VAP_PROFILE_NAME>	Wireless VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i>

Example

profile sonicpoint CorpVAPProfile

Syntax

no profile

Mode

Virtual Access Point

Description

Clear virtual access point profile.

Example

no profile

Syntax

80211r { enable | ft-over-ds | mix-mode }

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211r.

Options

<i>enable</i>	Enable IEEE802.11r enable.
<i>ft-over-ds</i>	Enable IEEE802.11r FT over DS.
<i>mix-mode</i>	Enable IEEE802.11r mix mode.

Example

80211r enable
80211r ft-over-ds 80211r mix-mode

Syntax

no 80211r { enable | ft-over-ds | mix-mode }

Mode

Description

Set SonicWave IEEE80211r.

Options

- enable*** Enable IEEE802.11r enable.
- ft-over-ds*** Disable IEEE802.11r FT over DS.
- mix-mode*** Disable IEEE802.11r mix mode.

Example

```
no 80211r
no 80211r ft-over-ds no 80211r mix-mode
```

Syntax

```
80211k neighbour-report
```

Mode

Description

Set SonicWave IEEE80211k.

Example

```
80211k neighbour-report
```

Syntax

```
no 80211k neighbour-report
```

Mode

Description

Set SonicWave IEEE80211k.

Example

```
no 80211k neighbour-report
```

Syntax

```
80211v { bss-trans-mgmt | wnm-sleep }
```

Mode

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Enable IEEE802.11v BSS transition management.

wnm-sleep Enable IEEE802.11v WNM sleep mode.

Example

80211v bss-trans-mgmt

Syntax

no 80211v { bss-trans-mgmt | wnm-sleep }

Mode

VAP Profile
Virtual Access Point

Description

Set SonicWave IEEE80211v.

Options

bss-trans-mgmt Disable IEEE802.11v BSS transition management.

wnm-sleep Disable IEEE802.11v WNM sleep mode.

Example

no 80211v bss-trans-mgmt

Syntax

show wireless [activities | discovered-access-points | ids | radio | stations | statistics | status [mix-mode { ap | station }] | virtual-access-point { { group <WIRELESS_VAP_GROUP_NAME> | groups | object <WIRELESS_VAP_NAME> | objects | profile <WIRELESS_VAP_PROFILE_NAME> | profiles } }] [{ pending-config | with-pending-config }]

Mode

All Modes

Description

Show wireless configuration.

Options

activities	Show wireless WLAN activities.
discovered-access-points	Show wireless discovered access points.
ids	Show wireless access point mode IDS settings.
radio	Show wireless radio settings.
stations	Show wireless access point mode connected stations.
statistics	Show wireless WLAN statistics.
status	Show wireless WLAN setting status.
mix-mode	Show wireless WLAN setting status.
ap	Show wireless ap status on mix mode.
station	Show wireless station status on mix mode.

<i>virtual-access-point</i>	Show wireless virtual access point configuration.
<i>group</i> <WIRELESS_VAP_GROUP_NAME>	Show virtual access point group configuration. Wireless VAP group name in the form: WORD or \"QUOTED STRING\". Example: <i>vapGroup</i>
<i>groups</i>	Show all virtual access point groups configuration.
<i>object</i> <WIRELESS_VAP_NAME>	Show wireless virtual access point object. Wireless VAP NAME in the form: WORD or \"QUOTED STRING\". Example: <i>vapObject</i>
<i>objects</i>	Show all wireless virtual access point objects.
<i>profile</i> <WIRELESS_VAP_PROFILE_NAME>	Show virtual access point profile configuration. Wireless VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i>
<i>profiles</i>	Show all wireless virtual access point profiles.
<i>pending-config</i>	Show pending configuration changes.
<i>with-pending-config</i>	View current configuration with pending changes included in the output.

Example

show wireless access-point

Syntax

```
show sonicpoint [ discovered-access-points [ sonicpoint <SONICPOINT_N_NAME> ] | fairnet [ { base | policies | policy {
direction { both | downlink | uplink } range <IPV4_HOST> <IPV4_HOST> interface <FAIRNET_INTERFACE> } } ] | firmware-management
| floor-plan <SONICPOINT_FLOOR_PLAN_NAME> | floor-plans | profile [ ac | n | ndr | wave2 ] <SONICPOINT_N_PROFILE_NAME> |
profile2 <SONICPOINT_N_PROFILE_NAME> | profiles [ { ac | n | ndr | wave2 } ] | rf { analysis [ { channel { { highly-interfered
| overloaded } } | score } ] | monitoring [ { discovered-threat-stations [ watch-list ] | statistics } ] } | rrm | sonicpoint
[ ac | n | ndr | wave2 ] <SONICPOINT_N_NAME> | sonicpoint2 <SONICPOINT_N_NAME> | sonicpoints [ { ac | n | ndr | wave2 } ] |
station { statistics [ { radio [ sonicpoint <SONICPOINT_N_NAME> [ station-mac <MAC> ] ] | sonicpoint <SONICPOINT_N_NAME> |
traffic [ sonicpoint <SONICPOINT_N_NAME> [ station-mac <MAC> ] ] } ] | status [ sonicpoint <SONICPOINT_N_NAME> [ station-mac
<MAC> ] ] } | statistics [ { radio [ sonicpoint <SONICPOINT_N_NAME> | sonicpoint <SONICPOINT_N_NAME> | traffic [ sonicpoint
<SONICPOINT_N_NAME> ] } ] | status [ sonicpoint <SONICPOINT_N_NAME> ] | virtual-access-point { { group <VAP_GROUP> | groups |
object <VAP_NAME> | objects | profile <VAP_PROFILE> | profiles } } | widp [ sensor-unit ] | wmm [ profile <WMM_PROFILE> ] ] [
{ pending-config | with-pending-config } ] ]
```

Mode

All Modes

Description

Show SonicPoint configuration.

Options

<i>discovered-access-points</i>	Show all SonicPoints discovered access points.
<i>sonicpoint</i> <SONICPOINT_N_NAME>	Show a specified SonicPoint discovered access points. SonicPointN name. Example: <i>mySonicpointn</i>
<i>fairnet</i>	Show FairNet configuration.
<i>base</i>	Show FairNet base settings.
<i>policies</i>	Show all FairNet policies.
<i>policy</i> <i>direction</i>	Show one specific FairNet policy. Specify direction.
<i>both</i>	Both.

downlink	Downlink (AP to client).
uplink	Uplink (client to AP).
range	Specify IP range.
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<IPV4_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
interface	Specify interface.
<FAIRNET_INTERFACE>	Fairnet interface name. Example: <i>X0</i>
firmware-management	Show SonicPoint firmware management configuration.
floor-plan	Show access point floor plan status.
<SONICPOINT_FLOOR_PLAN_NAME>	Word in the form: WORD or \"QUOTED STRING\". Example: <i>abc</i>
floor-plans	Show access point floor plans status.
profile	Show the specified SonicPointNs provisioning profiles.
ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2 profile.
<SONICPOINT_N_PROFILE_NAME>	SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i>
profile2	Show the specific sonicPoint provisioning profile.
<SONICPOINT_N_PROFILE_NAME>	SonicPointN provisioning profile name. Example: <i>mySonicpointnProfile</i>
profiles	Show available SonicPointNs provisioning profiles.
ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPointN.
ndr	SonicPointNDR.
wave2	SonicPoint ACWave2.
rf	Show SonicPoint RF monitoring and RF analysis information.
analysis	Show all SonicPoints RF analysis.
channel	Show SonicPoint each channel details.
highly-interfered	Show SonicPoint channel highly interfered by APs operating in the same channel as well as adjacent channels.
overloaded	Show SonicPoint channel overloaded by APs operating in the same channel.
score	Show all SonicPoints RF score.
monitoring	Show SonicPoint RF monitoring status or configuration.
discovered-threat-stations	Show discovered RF threat stations.
watch-list	Only stations in watch list group.
statistics	Show SonicPoint RF monitoring statistics information, including total data threats, total management threats, etc..
rrm	Show Radio Resource Management configuration.
sonicpoint	Show the specified SonicPointNs.

ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPoint N.
ndr	SonicPoint NDR.
wave2	SonicPoint ACWave2
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
sonicpoint2	Show the specific sonicPoint.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
sonicpoints	Show available SonicPointNs.
ac	SonicPoint ACe/ACi/N2/W2.
n	SonicPointN.
ndr	SonicPointNDR.
wave2	SonicPoint ACWave2.
station	Show all SonicPoints station status and statistics, status means some general information, including IP, SSID, AID, etc., statistics means statistical information, including radio and traffic statistics information.
statistics	Show all SonicPoints station statistics, including radio statistics and traffic statistics.
radio	Show all SonicPoints station's radio statistics information, including radio, channel, associations, disassociations, etc..
sonicpoint	Show a specified SonicPoint station's radio statistics information.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
station-mac	Show a specified SonicPoint station's radio statistics information.
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
sonicpoint	Show a specified SonicPoint station statistics.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
traffic	Show all SonicPoints station's traffic statistics information, including good packets, control packets, management packets, etc..
sonicpoint	Show a specified SonicPoint station's traffic statistics information.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
station-mac	Show a specified SonicPoint station's traffic statistics information.
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
status	Show all SonicPoints station status, including IP address, mac address, type, SSID, AID, etc..
sonicpoint	Show a specified SonicPoint station status.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
station-mac	Show a specified SonicPoint station status.
<MAC>	MAC address in the form: HH:HH:HH:HH:HH:HH OR HHHHHHHHHHHH. Example: <i>00:0C:F1:56:98:AD</i>
statistics	Show all SonicPoints statistics information, including radio statistics and traffic statistics.
radio	Show all SonicPoints radio statistics information, including radio, channel, associations, disassociations, etc..
sonicpoint	Show a specified SonicPoint radio statistics information.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
sonicpoint	Show a specified SonicPoint statistics.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
traffic	Show all SonicPoints traffic statistics information, including good packets, control packets, management packets, etc..
sonicpoint	Show a specified SonicPoint traffic statistics information.

<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
status	Show all SonicPoints status, including mac, IP, interface, zone, status, etc..
sonicpoint	Show a specified SonicPoint status.
<SONICPOINT_N_NAME>	SonicPointN name. Example: <i>mySonicpointn</i>
virtual-access-point	Show virtual access point(s), profile(s) or group(s).
group	Show specified virtual access point group.
<VAP_GROUP>	VAP group name in the form: WORD or \"QUOTED STRING\". Example: <i>vapGroup</i>
groups	Show all virtual access point groups.
object	Show specified virtual access point.
<VAP_NAME>	VAP NAME in the form: WORD or \"QUOTED STRING\". Example: <i>vapObject</i>
objects	Show all virtual access points.
profile	Show specified virtual access point profile configuration.
<VAP_PROFILE>	VAP profile name in the form: WORD or \"QUOTED STRING\". Example: <i>vapProfile</i>
profiles	Show all virtual access point profiles configuration.
widp	Show SonicPoint wireless intrusion detection and prevention configuration.
sensor-unit	Show SonicPoint WIDP sensor units information.
wmm	Show WiFi multimedia configuration.
profile	Show WiFi multimedia profile configuration.
<WMM_PROFILE>	WiFi multimedia profile name. Example: <i>abc</i>
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show sonicpoint
show sonicpoint floor-plan floorPlanName
show sonicpoint floor-plans
show sonicpoint profiles
show sonicpoint sonicpoints
show sonicpoint widp
show sonicpoint fairnet
show sonicpoint wmm
show sonicpoint rf monitoring
show sonicpoint rf analysis
show sonicpoint discovered-access-points
show sonicpoint station status
show sonicpoint station statistics
show sonicpoint status
show sonicpoint statistics
show sonicpoint rrm
```

Syntax

```
virtual-assist
```

Mode

Config

Description

Enter virtual assist configuration mode.

Example

Syntax

logout <CUSTOMER_ID>

Mode

Virtual Assist

Description

Logout specified virtual assist customer.

Options

<CUSTOMER_ID> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

logout myuser@acme.com

Syntax

assistance-code <WORD>

Mode

Virtual Assist

Description

Set virtual assist assistance code.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

assistance-code keyi0123

Syntax

no assistance-code

Mode

Virtual Assist

Description

Clear virtual assist assistance code.

Example

no assistance-code

Syntax

support-without-invitation

Mode

Virtual Assist

Description

Enable support without invitation.

Example

support-without-invitation

Syntax

no support-without-invitation

Mode

Virtual Assist

Description

Disable support without invitation.

Example

no support-without-invitation

Syntax

disclaimer <ROL>

Mode

Virtual Assist

Description

Set virtual assist disclaimer.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

disclaimer "Disclaimer message."

Syntax

no disclaimer

Mode

Virtual Assist

Description

Clear virtual assist disclaimer.

Example

no disclaimer

Syntax

customer-access-link <WORD>

Mode

Virtual Assist

Description

Set virtual assist customer access link.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
customer-access-link www.virtualassistaccess.com
```

Syntax

```
no customer-access-link
```

Mode

Virtual Assist

Description

Clear virtual assist customer access link.

Example

```
no customer-access-link
```

Syntax

```
link-on-portal-login
```

Mode

Virtual Assist

Description

Enable display virtual assist link from portal login.

Example

```
link-on-portal-login
```

Syntax

```
no link-on-portal-login
```

Mode

Virtual Assist

Description

Disable display virtual assist link from portal login.

Example

```
no link-on-portal-login
```

Syntax

```
technician-email-list <ROL>
```

Mode

Virtual Assist

Description

Set virtual assist technician e-mail list.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

```
technician-email-list myuser@acme.com
```

Syntax

```
no technician-email-list
```

Mode

Virtual Assist

Description

Clear virtual assist technician e-mail list.

Example

```
no technician-email-list
```

Syntax

```
invitation-subject <WORD>
```

Mode

Virtual Assist

Description

Set technician subject of invitation.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
invitation-subject \"%EXPERTNAME% has sent you a support invitation\"
```

Syntax

```
no invitation-subject
```

Mode

Virtual Assist

Description

Clear technician subject of invitation.

Example

no invitation-subject

Syntax

invitation-message <ROL>

Mode

Virtual Assist

Description

Set technician invitation message.

Options

<ROL> Remaining command line input.
Example: *line...*

Example

invitation-message "An assistance invitation has been generated for you"

Syntax

no invitation-message

Mode

Virtual Assist

Description

Clear technician invitation message.

Example

no invitation-message

Syntax

max-requests <UINT8>

Mode

Virtual Assist

Description

Set maximum requests.

Options

<UINT8> Integer in the form: D OR 0xHH.
Example: *123*

Example

max-requests 10

Syntax

limit-message <WORD>

Mode

Virtual Assist

Description

Set technician limit message.

Options

<WORD> Word in the form: WORD or \"QUOTED STRING\".
Example: *abc*

Example

```
limit-message "Maximum queue size reached, please try again later"
```

Syntax

```
no limit-message
```

Mode

Virtual Assist

Description

Clear technician limit message.

Example

```
no limit-message
```

Syntax

```
max-requests-one-ip <UINT16>
```

Mode

Virtual Assist

Description

Set maximum requests allowed from one IP.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: *123*

Example

```
max-requests-one-ip 5
```

Syntax

```
no max-requests-one-ip
```

Mode

Virtual Assist

Description

Set no limit requests allowed from one IP.

Example

```
no max-requests-one-ip
```

Syntax

pending-request-expiration <UINT16>

Mode

Virtual Assist

Description

Set time (in minutes) customers are allowed to remain in queue before being removed without being assisted by technician.

Options

<UINT16> Integer in the form: D OR 0xHHHH.
Example: 123

Example

pending-request-expiration 10

Syntax

no pending-request-expiration

Mode

Virtual Assist

Description

Clear expiration time customers are allowed to remain in queue before being removed without being assisted by technician.

Example

no pending-request-expiration

Syntax

deny-requests { *host* <IPV4_HOST> | *network* <IPV4_HOST> <IPV4_MASK> }

Mode

Virtual Assist

Description

Add address from which to deny requests from.

Options

host IP address.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168

network Network address and subnet mask.
<IPV4_HOST> IPV4 Address in the form: a.b.c.d.
Example: 192.168.168.168
<IPV4_MASK> IPV4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D.
Example: 255.255.255.0

Example

deny-requests host 10.10.10.1
deny-requests network 10.10.10.0 255.255.255.0

Syntax

```
no deny-requests { host <VIRTUAL_ASSIST_DENY_REQUESTS_HOST> | network <VIRTUAL_ASSIST_DENY_REQUESTS_HOST>
<VIRTUAL_ASSIST_DENY_REQUESTS_NETMASK> }
```

Mode

Virtual Assist

Description

Delete address from which to deny requests from.

Options

host	IP address.
<VIRTUAL_ASSIST_DENY_REQUESTS_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
network	Network address and subnet mask.
<VIRTUAL_ASSIST_DENY_REQUESTS_HOST>	IPv4 Address in the form: a.b.c.d. Example: <i>192.168.168.168</i>
<VIRTUAL_ASSIST_DENY_REQUESTS_NETMASK>	IPv4 netmask in decimal dotted or CIDR form: D.D.D.D OR /D. Example: <i>255.255.255.0</i>

Example

```
no deny-requests host 10.10.10.1
```

Syntax

```
show virtual-assist [ base | deny-requests | sessions ] [ { pending-config | with-pending-config } ]
```

Mode

All Modes

Description

Show virtual assist configuration.

Options

base	Show virtual assist base configuration.
deny-requests	Show virtual assist deny requests configuration.
sessions	Show virtual assist active customer sessions.
pending-config	Show pending configuration changes.
with-pending-config	View current configuration with pending changes included in the output.

Example

```
show virtual-assist
```

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS and SonicOSX E-CLI Reference Guide
Updated - March 2021
Software Version - 7
232-005460-00 Rev A

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035