SonicOS 7.0

Objects

Administration Guide

SONICWALL®

Contents

1

MATCH OBJECTS

Match objects represent the set of conditions which must be matched for actions to take place. You can create objects once and re-use them across the SonicOS interface.

The following table identifies which match object features are available in Classic Mode and Policy Mode.

Match Object Feature	Classic Mode	Policy Mode
Zones	Yes	Yes
Addresses	Yes	Yes
Services	Yes	Yes
URI Lists	Yes	Yes
Schedules	Yes	Yes
Dynamic Group	Yes	Yes
Email Addresses	Yes	Yes
Match Objects	Yes	
Countries		Yes
Applications		Yes
Web Categories		Yes
Websites		Yes
Match Patterns		Yes
Custom Match		Yes

1

Zones

A zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying Access Rules (Classic Mode) or Security Policies (Policy Mode) as traffic passes from one zone to another zone. Zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same Access Rules (Classic Mode) or Security Policies (Policy Mode) to them, instead of having to write the same policy for each interface.

Topics:

How Zones Work

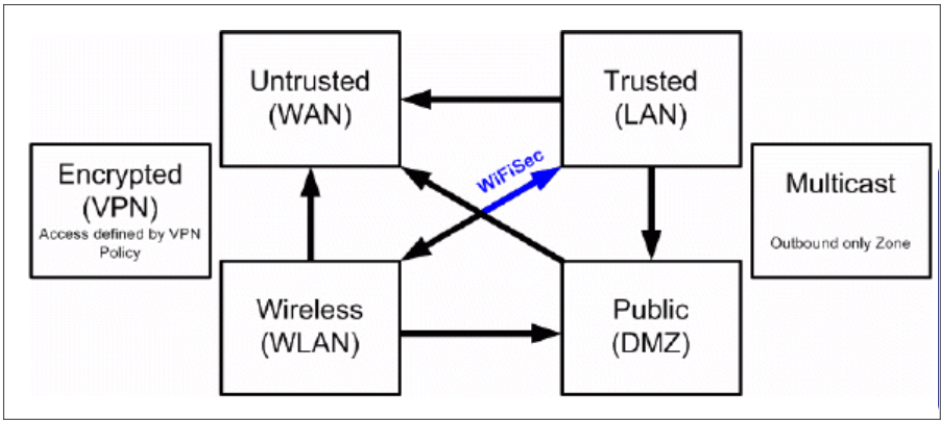
An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a door person on the way out of each room. This door person is the inter-zone/intra-zone security policy, and the door person's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (for example, the security policy allows them in), they can leave the room through the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit,

depending upon how they have been told to do so (for example, only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the door person (the security policy) to point out which person in the other group is the one with whom they wish to speak. The door person has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people want to visit remote offices, and people might arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The door person can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.



Default Zones

ⓘ | **NOTE:** The default zones on your firewall depends on the device.

The default security zones on the SonicWall Security Appliance are not modifiable:

This Zone	Security Type	Has this function
LAN	Trusted	Consist of multiple interfaces, depending on your network design. Even though each interface has a different network subnet attached to it, when grouped together, they can be managed as a single entity.
WAN	Untrusted	Consist of multiple interfaces. If you are using the Security Appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
MGMT	Management	Used for appliance management and includes only the MGMT interface. Interfaces in other zones can also be enabled for SonicOS management, but the MGMT zone or interface provides the added security of a separate zone just for management.
DMZ	Public	Normally used for publicly accessible servers and can consist of one to four interfaces, depending on your network design.
VPN	Encrypted	A virtual zone used for simplifying secure and remote connectivity.
SSLVPN	Sslvpn	Used for secure remote access using the SonicWall NetExtender client.
MULTICAST	Untrusted	Provides support for IP multicasting, which is a method for sending packets from a single source simultaneously to multiple hosts.
WLAN	Wireless	WLAN is available only in Classic Mode. Provides support to SonicWall SonicPoints and SonicWaves. Any unassigned interface can be added to WLAN, allowing the administrator to discover, provision, monitor, and protect the wireless traffic access through SonicPoints and SonicWaves connected to the WLAN zone. The WLAN zone supports: • SonicWall Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints and SonicWaves • SonicWall Simple Provisioning Protocol (SSPP) to configure SonicPoints and SonicWaves using profiles • Wireless and guest service configurations

ⓘ | **NOTE:** Even though you can group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

ⓘ | **NOTE:** The security types of a zone depend on the device.

Each zone has a security type, which defines the level of trust given to that zone.

Trusted	Provides the highest level of trust. The least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the Security Appliance. The LAN zone is always Trusted.
Management	ⓘ	**NOTE:** This type is available only in Policy Mode. Provides the highest level of trust. Unique to the MGMT zone and MGMT interface.
Encrypted	Used exclusively by the VPN and SSLVPN zones. All traffic to and from an Encrypted zone is encrypted.
Public	Offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the Security Appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default, traffic from DMZ to LAN is denied, but traffic from LAN to ANY is allowed. This means only LAN-initiated connections have traffic between DMZ and LAN. The DMZ only has default access to the WAN, not the LAN.
Untrusted	Represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the Security Appliance. By the default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.
Wireless	ⓘ	**NOTE:** This type is available only in Classic Mode. Applied to the WLAN zone or any zone where the only interface to the network consists of SonicWall SonicPoint and SonicWave devices. Wireless security type is designed specifically for use with SonicPoints and SonicWaves. Placing an interface in a Wireless zone activates SDP and SSPP on that interface for automatic discovery and provisioning of SonicPoints and SonicWaves. Only traffic that passes through a SonicPoint or SonicWave is allowed through a Wireless zone, all other traffic is dropped.
SSLVPN	Provides secure remote access to the network using the NetExtender client. NetExtender allows remote clients seamless access to resources on your local network.

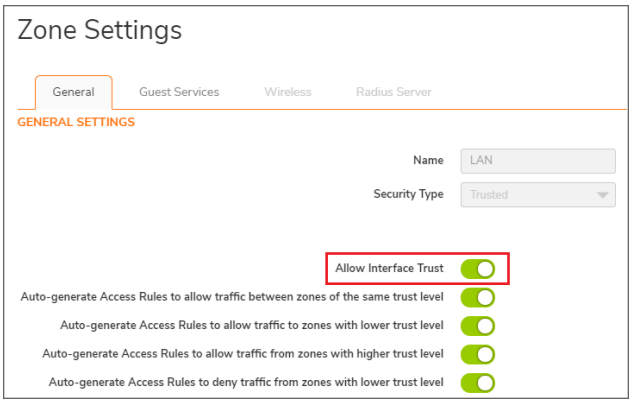
Allow Interface Trust

This option is available only in Classic Mode.

Enabling **Allow Interface Trust** option of a Zone automates the creation of Access Rules to allow traffic flow between the interface of a zone instance.

Example:

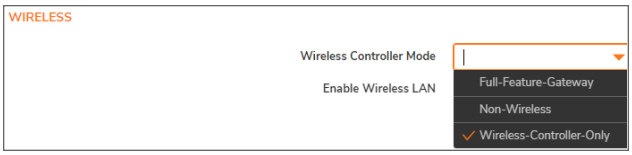
If the LAN zone has both the **LAN** and **X3** interfaces assigned to it, enabling **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.



Effect of Wireless Controller Modes

ⓘ | **NOTE:** This section is applicable only for Classic Mode.

Setting of the **Wireless Controller Mode** on the **DEVICE | Settings> Administration** page affects the **OBJECT | Match Objects > Zones** page.



Topics:

- Effects of Enabling Non-Wireless Controller Mode
- Effects of Enabling Wireless Controller Mode

Effects of Enabling Non-Wireless Controller Mode

ⓘ | **NOTE:** This section is applicable only for Classic Mode.

Selecting the **Wireless Controller Mode** as **Non-Wireless** on the **DEVICE | Settings> Administration** affects the **OBJECT | Match Objects > Zones** page. Attempts to enable or delete the affected features are denied.

- Editing or deleting wireless zones are not allowed on the **OBJECT | Match Objects > Zones** page.
  - When you try to edit, you get **Read only** error.
  - **Delete** icon for wireless zones is unavailable.
- Internal wireless zones are disabled.
- You are not allowed to create a new zone with **Wireless** security type.

Effects of Enabling Wireless Controller Mode

ⓘ | **NOTE:** This section is applicable only for Classic Mode.

Selecting the **Wireless Controller Mode** as **Wireless-Controller-Only** on the **DEVICE | Settings> Administration** affects the **OBJECT | Match Objects > Zones** page. Attempts to enable or delete the affected features are denied.

- The **Edit** and **Delete** icons for VPN and SSL VPN zones are unavailable on the **OBJECT | Match Objects > Zones** page.
- Any attempt to enable a zone with VPN and/or SSL VPN results in an error.
- You are not allowed to create a new zone with **VPN** or **SSL VPN** security type.

Zones Overview

Topics:

- The Zones Page
- Adding a New Zone
- Cloning a Zone
- Editing a Zone
- Deleting Custom Zones

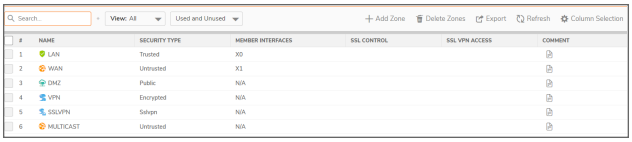
The Zones Page

The **Zones** page displays a list of default zones as well as custom zones created for the SonicWall Security Appliance.

From the **Zones** page, you can:

- Filter the table data with possible combinations
- Add, modify, and delete zones
- Clone from an exiting zone to create a new zone
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in
- View the Member Interfaces added to the Zones
- View the Security Services enabled on the Zones
- View the comment added for Zones

Policy Mode



Classic Mode

Topics:

Interpreting the Zones Table

Interpreting the Zones Table

Display of the Zones table depends on customization of the **Columns**. For more information refer to Common Actions with Objects Table.

Table Column	Description
NAME	The **Name** column shows name of the zones. **LAN**, **WAN**, **WLAN**, **DMZ**, **VPN**, **SSLVPN**, **MGMT**, **MULTICAST**, and **Encrypted** are default zones. For more information, refer to Default Zones. ⓘ **NOTE:** You can modify services of a default zones but you cannot modify name of the default zones.
SECURITY TYPE	The **Security Type** column shows the type of security selected for the zone from **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**. For more information, refer to Security Types.
MEMBER INTERFACES	The **Member Interfaces** column shows the interfaces that are members of the zone.

Selected check boxes in the **Zone Settings** table gives you an overview of Security Services enabled for the Zone.

ⓘ **NOTE:** Only **CLIENT AV**, **SSL CONTROL and SSL VPN ACCESS** services are available for Policy Mode.

Table Column	Description
INTERFACE TRUST	**Allow Interface Trust** is enabled for the zone. For more information, refer to Allow Interface Trust.
CLIENT AV	SonicWall Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Client Anti-Virus manages an anti-virus client application on all clients on the zone.
CLIENT CF	Client Content Filtering services are enabled.
GATEWAY AV	SonicWall Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Gateway Anti-Virus manages the anti-virus service on the firewall.
ANTI-SPYWARE	SonicWall Anti-Spyware detection and prevention is enabled for traffic going through interfaces in the zone.
IPS	SonicWall Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
APP CONTROL	App Control Service is enabled for traffic coming in and going out the zone.

Table Column	Description
SSL CONTROL	SSL Control is enabled for traffic coming in and going out the zone. All new SSL connections initiated from that zone are now subject to inspection.
SSL VPN ACCESS	SSL VPN secure remote access is enabled for traffic coming in and going out of the zone.
DPI SSL CLIENT	Granular DPI-SSL on a per-zone basis is enabled rather than a global basis for DPI-SSL clients.
DPI SSL SERVER	Granular DPI-SSL on a per-zone basis is enabled rather than global basis for DPI-SSL servers.

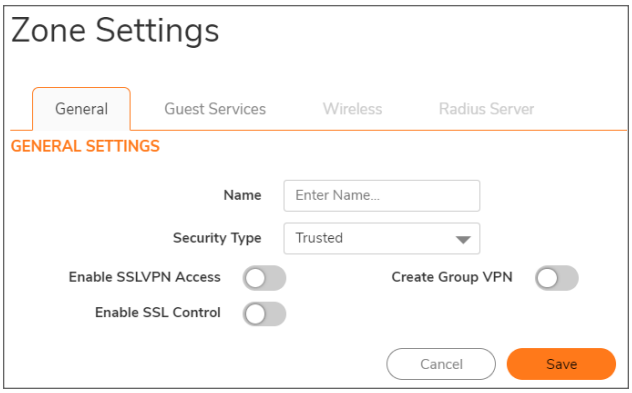
Adding a New Zone

Topics:

Adding a New Zone in Policy Mode

To add a new zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Click the **Add Zone** icon.



3. Type a **Name** for the new zone.
4. Select the **Security Type**.

Trusted	To create a zone with the highest level of trust, such as internal LAN segments.
Public	To create a zone with a lower level of trust requirements, such as a DMZ interface.
SSLVPN	To create a zone for interfaces on which Content Filtering, Client AV enforcement, and Client CF services are enabled. ⓘ **NOTE: Enable SSLVPN Access** and **Create Group VPN** options are not available for **SSLVPN** Security Type.

5. Set the toggle keys for security services as required.

Toggle key	Security Service
Enable SSLVPN Access	To enable SSL VPN secure remote access on the zone.

Toggle key	Security Service
Create Group VPN	To create a SonicWall Group VPN Policy for this zone automatically. You can view and customize the Group VPN Policy on **NETWORK | SSLVPN > Server Settings** page. ⓘ **NOTE:** • **Enable SSLVPN Access** option is not available if **SSLVPN** is selected as Security Type. • The **Create Group VPN** option is available until **SSLVPN** is selected as Security Type. If the Security Type is changed to any other type, the **Create Group VPN** option becomes available. △ **CAUTION: Disabling Create Group VPN removes any corresponding Group VPN policy.** Disabling Group VPN for WAN or WLAN VPN policies, deletes all VPN policies. Re-enabling the **Create Group VPN** option automatically creates a new, enabled VPN policy. Disabling VPN policies globally does not delete auto-rules. If you do not want VPN policies at all, globally disable VPN, and delete all policies that correlate with VPN. WAN or WLAN Group VPN policies are disabled by the default when the firewall is booted with the factory default. For more information about connectivity options, refer to the *SonicOS Connectivity*.
Enable SSL Control	To enable SSL Control on the zone. All new SSL connections initiated from the zone are now subject to inspection. ⓘ **NOTE:** Make sure that the SSL Control is enabled globally on **NETWORK | Firewall > SSL Control** page.

6. Click **Save**.

   The new zone is now added to the Security Appliance.

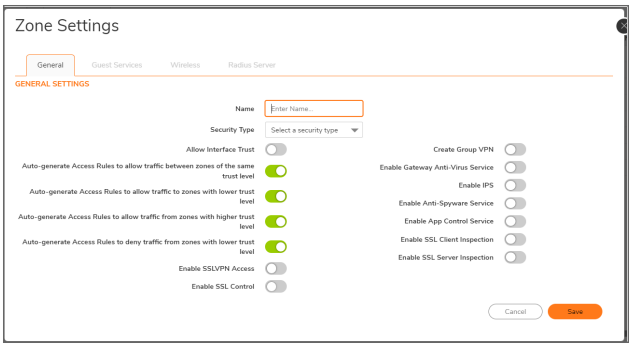
Adding a New Zone in Classic Mode

To add a new zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Click the **Add Zone** icon.

   The **Zone Settings** page enables the below listed options by the default on the **General** tab, but these comes into effect only when **Allow Interface Trust** is enabled.

   - **Auto-generate Access Rules to allow traffic between zones of the same trust level**
   - **Auto-generate Access Rules to allow traffic to zones with lower trust level**
   - **Auto-generate Access Rules to allow traffic from zones with higher trust level**
   - **Auto-generate Access Rules to deny traffic from zones with lower trust level**



3. Type a **Name** for the new zone.
4. Select the **Security Type**.

Trusted	To create a zone with the highest level of trust, such as internal LAN segments.
Public	To create a zone with a lower level of trust requirements, such as a DMZ interface.
Wireless	To create a zone for WLAN interface.
SSLVPN	To create a zone for interfaces on which Content Filtering, Client AV enforcement, and Client CF services are enabled. **NOTE: Enable SSLVPN Access** and **Create Group VPN** options are not available for **SSLVPN** Security Type.

5. Enable **Allow Interface Trust** to allow intra-zone communications.

   An Access Rule allowing traffic to flow between the interfaces of a Zone instance is created automatically.
6. Set the toggle keys to generate access rules automatically as required.

NOTE:
- By the default, these options are enabled.
- For more information, refer to **Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

Toggle key	To allow traffic between	Example
Auto-generate Access Rules to allow traffic between zones of the same trust level	This zone and other zones of equal trust	*CUSTOM_LAN > CUSTOM _LAN or CUSTOM_LAN > LAN*
Auto-generate Access Rules to allow traffic to zones with lower trust level.	This zone and other zones of lower trust	*CUSTOM_LAN > WAN or CUSTOM_ LAN > DMZ*
Auto-generate Access Rules to allow traffic from zones with higher trust level.	This zone and other zones of higher trust	*LAN > CUSTOM_DMZ or CUSTOM_ LAN > CUSTOM_DMZ*
Auto-generate Access Rules to deny traffic from zones with lower trust level	This zone and zones of lower trust	*WAN > CUSTOM_LAN* or *DMZ > CUSTOM_LAN*

7. Set the toggle keys for security services as required.

Toggle key	Security Service
Enable SSLVPN Access	To enable SSL VPN secure remote access on the zone.
Enable SSL Control	To enable SSL Control on the zone. All new SSL connections initiated from the zone are now subject to inspection. ⓘ **NOTE:** Make sure that the SSL Control is enabled globally on **NETWORK | Firewall > SSL Control** page.
Create Group VPN	To create a SonicWall Group VPN Policy for this zone automatically. You can view and customize the Group VPN Policy in **NETWORK | SSLVPN > Server Settings** page. ⓘ **NOTE:** • **Enable SSLVPN Access** option is not available if **SSLVPN** is selected as Security Type. • The **Create Group VPN** option is available until **SSLVPN** is selected as Security Type. If the Security Type is changed to any other type, the **Create Group VPN** option becomes available. △ **CAUTION: Disabling Create Group VPN removes any corresponding Group VPN policy.** Disabling Group VPN for WAN or WLAN VPN policies, deletes all VPN policies. Re-enabling the **Create Group VPN** option automatically creates a new, enabled VPN policy. Disabling VPN policies globally does not delete auto-rules. If you do not want VPN policies at all, globally disable VPN, and delete all policies that correlate with VPN. WAN or WLAN Group VPN policies are disabled by the default when the firewall is booted with the factory default. For more information about connectivity options, refer to the *SonicOS Connectivity*.
Enable Gateway Anti-Virus Service	To enforce gateway anti-virus protection on your Security Appliance for all clients connecting to this zone. SonicWall Gateway Anti-Virus manages the anti-virus service on the Security Appliance.
Enable IPS	To enforce intrusion detection and prevention on multiple interfaces in the same Trusted, Public, or WLAN zones.
Enable Anti-Spyware Service	To enforce anti-spyware detection and prevention on multiple interfaces in the same Trusted or Public security type for WLAN zones.
Enable App Control Service	To enforce application control policy services on multiple interfaces in the same Trusted or Public security type for WLAN zones. For more information about App Control, refer to SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

Toggle key	Security Service
Enable SSL Client Inspection	To enable granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL clients.
Enable SSL Server Inspection	To enable granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL servers.

8. Click **Save**.

   The new zone is now added to the Security Appliance.

Configuring a Zone for Guest Access

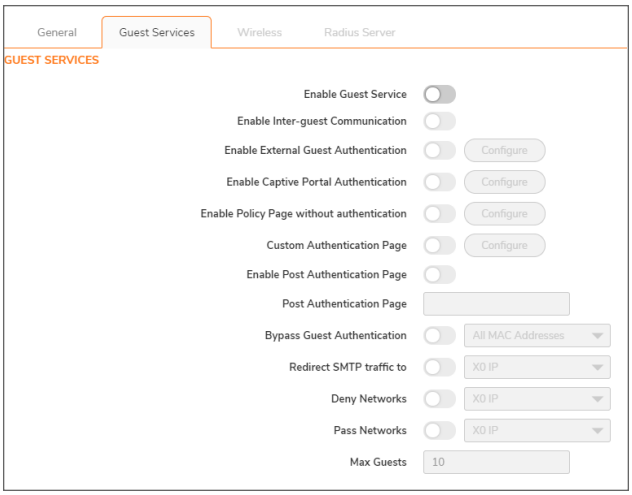
ⓘ **IMPORTANT:** You cannot configure guest access for an **Untrusted**, **Encrypted**, **SSL VPN**, or **Management** zone.

SonicWall user Guest Services provide an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to wireless or wired users on the WLAN, LAN, DMZ, public, or semi-public zone of your choice.

To configure Guest Services:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone in the **Zones** table and click the **Edit** icon to add Guest Services.
3. Click the **Guest Services** tab.

   By the default, all the options are disabled for Guest Services.



4. **Enable Guest Services** to make the guest services options available for selection.
5. Set the toggle keys and configuration for **Guest Services** as follows.

Enable inter-guest communication	Allows guests to communicate directly with other users who are connected to this zone.
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. Selecting this option makes **Configure** available. ⓘ **NOTE:** When **Enable External Guest Authentication** is selected, the following options become unavailable: • Enable Captive Portal Authentication • Enable Policy Page without authentication • Custom Authentication Page
Enable Captive Portal Authentication	This option is available only in Classic Mode. You can enable this option only when **Enable External Guest Authentication** option is disabled. Allows you to create a customized login page with RADIUS authentication. Selecting this option makes **Configure** available. For more information about configuring **Enable Captive Portal Authentication**, refer to the Configuring a Zone for Captive Portal Authentication with RADIUS. ⓘ **NOTE: Enable Policy Page without authentication** is unavailable for **Enable Captive Portal Authentication**.
Enable Policy Page without authentication	Directs users to a guest services usage policy page when they first connect to a SonicPoint or SonicWave in the WLAN zone. Guest users are authenticated by accepting the policy instead of providing a user name and password. Selecting this option makes **Configure** available. Click **Configure** to set up a HTML customizable policy usage page. For more information, refer to the Configuring a Zone for Customized Policy Message. ⓘ **NOTE:** When you **Enable Policy Page without authentication** option, **Enable Captive Portal Authentication** option gets disabled automatically.
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to the network. Selecting this option makes **Configure** available. Click **Configure** to set up a custom authentication page. For more information, refer to the Configuring a Zone for Customized Login Page.
Enable Post Authentication Page	Directs users to the specified page immediately after successful authentication. Selecting this option makes **Post Authentication Page** field available.
Post Authentication Page	Enter a URL for the post-authentication page.

Bypass Guest Authentication	Allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the authentication process, allowing wireless users unrestricted wireless Guest Services without requiring authentication. When **Bypass Guest Authentication** is enabled, drop-down menu becomes available: • **All MAC Addresses** (default) • An Address Object • An Address Group • Create new MAC object • Create new MAC object group **NOTE:** This feature should only be used when unrestricted Guest Service access is desired or when another device upstream is enforcing authentication.
Redirect SMTP traffic to	Redirects incoming SMTP traffic on this zone to a SMTP server you specify. When **Redirect SMTP traffic to** is enabled, drop-down menu becomes available: • An Address Object • Create new address object
Deny Networks	Blocks traffic to the selected networks. When **Deny Networks** is enabled, drop-down menu becomes available • An Address Object • An Address Object group • Create new address object • Create new address object group
Pass Networks	Allows traffic through the Guest Service-enabled zone to the selected networks automatically. When **Pass Networks** is enabled, drop-down menu becomes available: • An Address Object • An Address Object group • Create new address object • Create new address object group
Max Guests	Specifies the maximum number of guest users allowed to connect to this zone. The minimum number is 1, the maximum number is 4500, and the default number is **10**.
Wireless Zone Guest Services Options	Displays only for the WLAN zone or for a custom zone with a **Security Type** of **Wireless**.
Enable Dynamic Address Translation	Grants access to non-DHCP guests.

6. Click **Save** to apply these settings to this zone.

Configuring a Zone for Open Authentication and Social Login

SonicOS supports Open Authentication (OAuth) and Social Login:

- Oauth assists users in sharing data between applications
- Social Login simplifies the login process for various social media

For information about configuration, refer to:

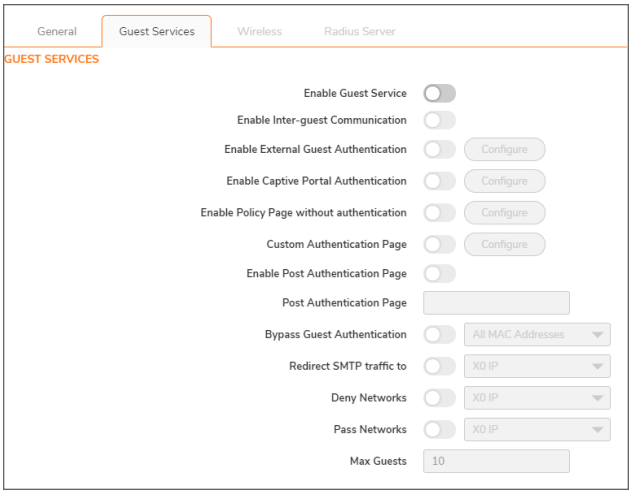
- Configuring a Zone for Captive Portal Authentication with RADIUS
- Configuring a Zone for Customized Policy Message
- Configuring a Zone for Customized Login Page

Configuring a Zone for Captive Portal Authentication with RADIUS

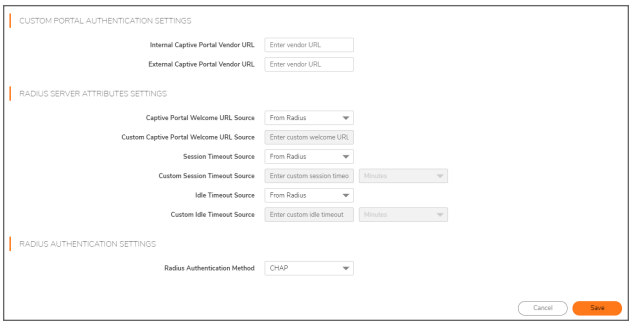
ⓘ | **NOTE:** This feature is available only in Classic Mode.

To configure captive portal authentication with RADIUS:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone in the **Zones** table and click the **Edit** icon to add Guest Services.
3. Click the **Guest Services** tab.
   By the default, all the options are disabled for Guest Services.



4. **Enable Guest Services** to make the guest services options available for selection.
5. **Enable Captive Portal Authentication**.
6. Click **Configure**.



7. Enter the **CUSTOM PORTAL AUTHENTICATION SETTINGS** details:
   a. The **Internal Captive Portal Vendor URL**
   b. The **External Captive Portal Vendor URL**

8. Leave the attributes to default or set the custom attributes in the **RADIUS SERVER ATTRIBUTES SETTINGS** section. Set the attributes setting:
   - **From Radius** leaves the attribute settings as the default.
   - **Custom** allows to customize the attribute settings according to the below table.

Attribute Name	Setting	
	From Radius	**Custom**
Captive Portal Welcome URL Source	Default	Enter the welcome URL in the **Custom Captive Portal Welcome URL** field.
Session Timeout Source	Default	1. Enter the limit in the field. 2. Select the type of timeout from the drop-down menu: • Minutes • Hours • Days (default)
Idle Timeout Source	Default	

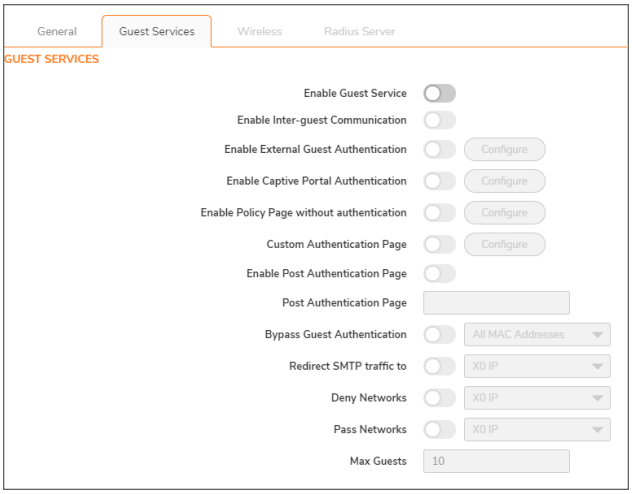
9. Select the **Radius Authentication Method** in the **Radius Authentication Settings** section:
   - CHAP (default)
   - PAP – Encrypted
   - PAP – ClearText
10. Click **Save**.

Configuring a Zone for Customized Policy Message

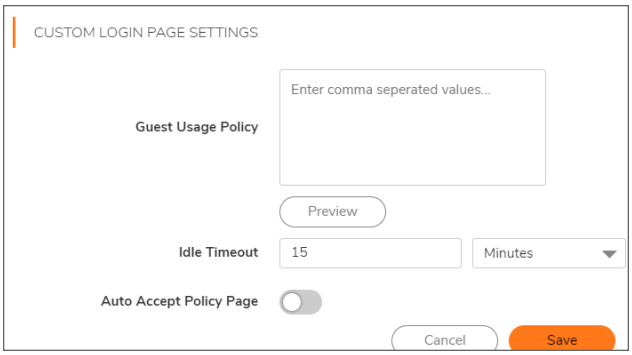
To configure a customized policy message:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone in the **Zones** table and click the **Edit** icon to add Guest Services.

3. Click the **Guest Services** tab.
   By the default, all the options are disabled for Guest Services.



4. **Enable Guest Services** to make the guest services options available for selection.
5. **Enable Policy Page without authentication**.
6. Click **Configure**.

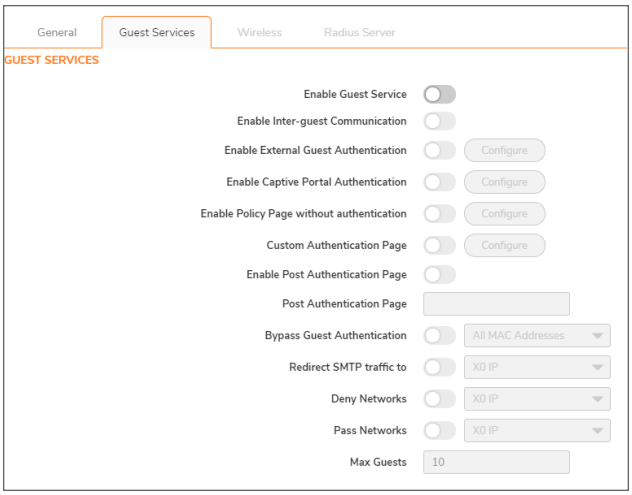


7. Enter the **Guest Usage Policy**.
   The text may include HTML formatting.
8. Click **Preview** to preview the entered policy message.
9. Enter the **Idle Timeout** value.
10. Select the type of timeout:
    - Seconds
    - Minutes (default)
    - Hours
    - Days
11. Click **Save**.

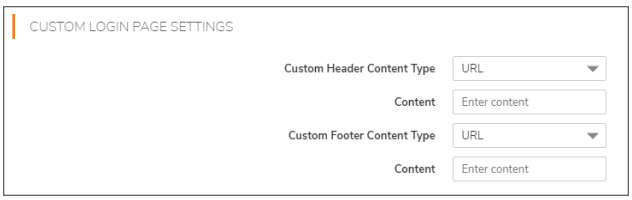
Configuring a Zone for Customized Login Page

To configure a customized login page:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone in the **Zones** table and click the **Edit** icon to add Guest Services.
3. Click the **Guest Services** tab.
   By the default, all the options are disabled for Guest Services.



4. **Enable Guest Services** to make the guest services options available for selection.
2. Enable **Custom Authentication Page**.
3. Click **Configure**.



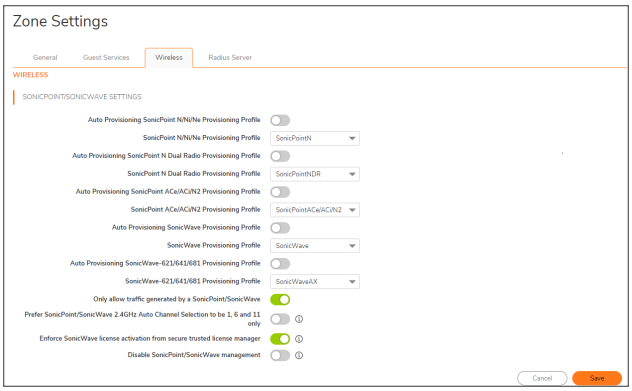
4. Select the content type, **URL** or **Text** for **Custom Header Content Type**.
5. Enter the URL or Text in the **Content** field.
6. Repeat the above two steps for **Custom Footer Content Type**.
7. Click **Save**.

Configuring the WLAN Zone

NOTE: This feature is available only in Classic Mode. **Wireless** tab is available only for the zones created with Security Type as **Wireless**.

To configure a WLAN zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Do one of the following:
   - Add a new zone
     1. Click the **Add Zone** icon.
     2. Type a **Name** for the new zone.
     3. Select the **Security Type** as **Wireless**.
   - Edit an existing zone.
     Hover over the wireless zone in the **Zones** table and click the **Edit** icon.
3. Click the **Wireless** tab.



4. In the **SonicPoint/SonicWave Settings** section, set the provisioning profiles.

   NOTE:
   - Enable the required **Auto provisioning** options to allow automatic provisioning of SonicPoints or SonicWaves attached to the profile when the profile is modified.
   - Whenever a SonicPoint or SonicWave connects to this zone, it is provisioned automatically by the settings in the SonicPoint or SonicWave Provisioning Profile, unless you have individually configured it with different settings.

Provisioning Profile	Rule	Default Setting
SonicPointN/Ni/Ne Provisioning Profile	To apply to all SonicPointN/Ni/Nes connected to this zone.	SonicPointN

Provisioning Profile	Rule	Default Setting
SonicPoint N Dual Radio Provisioning Profile	To apply to all SonicPointNDRs connected to this zone.	SonicPointNDR
SonicPointACe/ACi/N2 Provisioning Profile	To apply to all SonicPointACe/ACi/N2s connected to this zone.	SonicPointACe/ACi/N2
SonicWave Provisioning Profile	To apply to all SonicPointWaves connected to this zone.	SonicWave
SonicWave-621/641/681 Provisioning Profile	To apply to all SonicWave-621/641/681 connected to this zone.	SonicWaveAX

5. Clear **Only allow traffic generated by a SonicPoint/SonicWave** to allow any traffic on your WLAN zone regardless of whether the traffic is from a wireless connection.

   Only allow traffic generated by a SonicPoint/SonicWave is selected by the default. You can leave it selected to allow only traffic from SonicWall SonicPoints to enter the WLAN zone interface. This allows maximum security of your WLAN.

   For more information on:

   - Guest Services configuration, refer to Configuring a Zone for Guest Access.
   - RADIUS server configuration, refer to Configuring the RADIUS Server.

6. Select **Prefer SonicPoint/SonicWave 2.4Hz Auto Channel Selection to be 1, 6 and 11 only** if the preferred auto channel selection is 1, 6, or 11.
7. Select **Enforce SonicWave license activation from secure trusted license manager** to enforce license activation from a secure trusted license manager.

   CAUTION: Manual license keyset input is not allowed. Change this setting only under the direction of Technical Support.

8. Select **Disable SonicPoint/SonicWave management** to disable all management capabilities on this WLAN.
9. Click **Save**.

Configuring the RADIUS Server

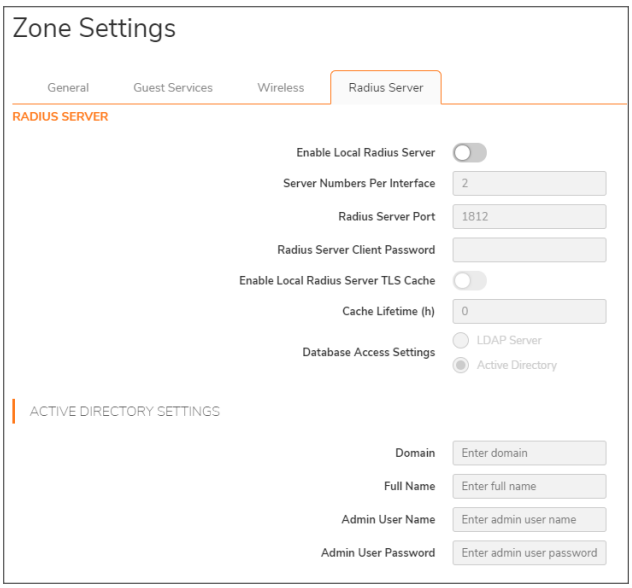
NOTE: This feature is available only in Classic Mode. **Radius Server** tab is available only for the zones created with Security Type as **Wireless**. It can be enabled or disabled based on the device.

To configure RADIUS server:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Do one of the following:

- Add a new zone
    1. Click the **Add Zone** icon.
    2. Type a **Name** for the new zone.
    3. Select the **Security Type** as **Wireless**.
- Edit an existing zone.
  Hover over the wireless zone in the **Zones** table and click the **Edit** icon

3. Click **Radius Server** tab.

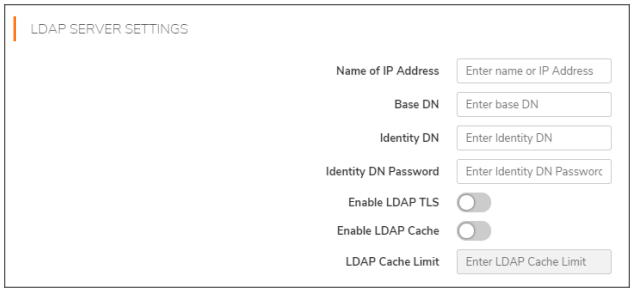
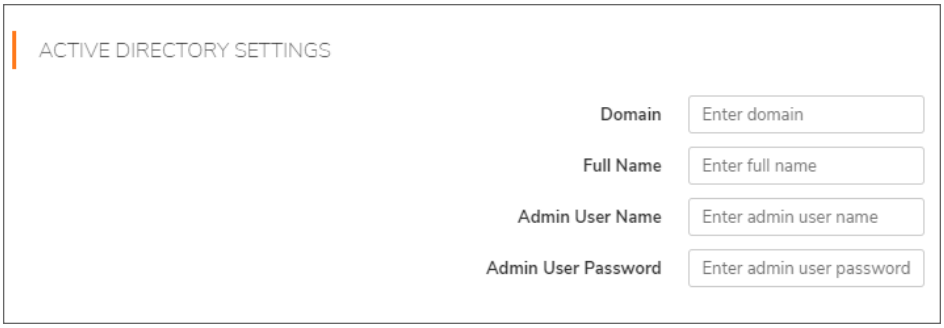


4. **Enable Local Radius Server** to make the Radius Server options available for selection.
5. Set the Radius Server:

Field	Default Value	Additional
Server Numbers Per Interface	2	Minimum number is 1, and maximum is 512
Radius Server Port	1812	
Radius Client Password	Enter the client password	

6. **Enable Local Radius Server TLS Cache** to enter the **Cache Lifetime(h)**.
   The minimum and default is **1** hour, and the maximum is 99999 hours.

7. Select the **Database Access Settings** method and define the settings.

Database Access Settings	Settings
LDAP Server	1. Enter the **LDAP SERVER SETTINGS**: • Name or IP address in the **Name of IP Address** field • Base distinguished name in the **Base DN** field • Identity distinguished name in the **Identity DN** field • Identity distinguished name password in the **Identity DN Password** field 2. **Enable LDAP TLS** to enable LDAP Transport Layer Security (TLS). 3. **Enable LDAP Cache** to enter **LDAP Cache Limit** in seconds. The minimum is 1, the maximum is 99999, and the default is **86400**. 
Active Directory	Enter the **ACTIVE DIRECTORY SETTINGS**: • **Domain** name • Active Directory **Full Name** • **Admin User Name** • **Admin User Password** 

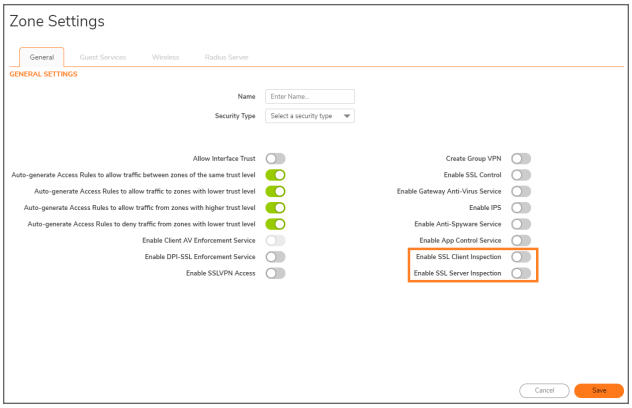
8. Click **Save**.

Configuring DPI-SSL Granular Control per Zone

DPI-SSL granular control allows you to enable DPI-SSL on per-zone basis rather than globally. You can enable both DPI-SSL Client and DPI-SSL Server per zone. For more information, refer to SonicOS 7.0 DPI SSL Administration Guide.

To configure DPI-SSL granular control per zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone in the **Zones** table and click the **Edit** icon.
3. Select **Enable SSL Client Inspection** and **Enable SSL Server Inspection** options to enable DPI-SSL Client and DPI-SSL Server per zone.



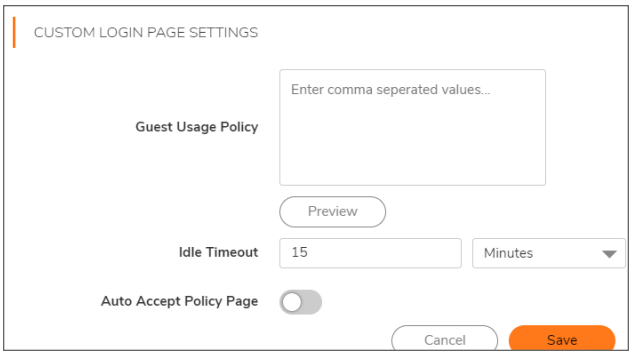
4. Click **Save**.

Enabling Automatic Redirection to the User-Policy Page

SonicOS allows you to redirect a guest automatically to your guest-user policy page. If you enable this feature, also known as the zero-touch policy page redirection, the guest user is redirected automatically to your guest-user policy page. If you disable the feature, the guest must click **Accept**.

To enable automatic redirection to the user-policy page:

1. Configure a zone according to Configuring a Zone for Customized Policy Message.
2. Enable **Auto Accept Policy Page** to redirect a guest automatically to your guest-user policy page.



3. Click **Save**.

Cloning a Zone

ⓘ | **NOTE:** You can clone from all custom zones and some of the default zones.

To clone from an existing zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone from which you want to clone and click the **Clone** icon.
   This creates a duplicate of the zone, which allows you to create a new zone with the same settings.
3. Make the necessary changes.
   For more information, refer to Adding a New Zone.
4. Click **Save**.

Editing a Zone

ⓘ | **NOTE:**

- You can modify services of the default zones but you cannot modify Security Type of the default zones. For some of the default zones, you can modify the name also.
- Check boxes of the default zones in the Zones table are unavailable for selection.
- For the complete list of the default zones, refer to Default Zones.

To edit a zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the zone to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding a New Zone.
4. Click **Save**.

Deleting Custom Zones

NOTE:

- You cannot delete the default zones. For the complete list of the default zones, refer to the Default Zones.
- Check boxes of the default zones in the Zones table are unavailable for selection.
- You cannot delete a zone if it is in use by Rule.
- You can delete only custom zones.

To delete a custom zone:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all custom zones:

1. Navigate to **OBJECT | Match Objects > Zones**.
2. Do one of the following:
   - Select check boxes of the objects to be deleted.
   - Select the check box in the table header to select all custom objects.
3. Click the **Delete Zones** icon on top of the table.
4. Do one of the following:
   1. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
   2. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

2

Addresses

Address objects (AOs) allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. While more effort is involved in creating an address object than in simply entering an IP address, address objects were implemented to complement the management scheme of SonicOS, providing the following characteristics:

- **Zone Association**

  When defined, host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as access rules (Classic Mode) or security policies (Policy Mode)) is only used referentially. The functional application are the contextually accurate populations of address object drop-down menus and the area of VPN access definitions assigned to users and groups. When AOs are used to define VPN access, the access rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the host AO, *192.168.168.200* , belonging to the LAN zone was added to VPN access for the *Trusted Users* user group, the auto-created access rule would be assigned to the VPN LAN zone.

- **Management and Handling**

  The versatile family of address objects types can be easily used throughout the SonicOS interface, allowing for handles (for example, when defining access rules (Classic Mode) or security policies (Policy Mode)) to be quickly defined and managed. The ability to simply add or remove members from address groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.

- **Reusability**

  Objects only need to be defined once and can then be easily referenced as many times as needed.

For example, take an internal web server with an IP address of *67.115.118.80*. Rather than repeatedly typing in the IP address when constructing access rules or NAT policies, you can create a single entity called *My Web Server* as a host address object with an IP address of *67.115.118.80*. This address object, **My Web Server**, can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs address objects as a defining criterion.

Topics:

Addresses Page

The **Addresses** page has two tabs and displays a list of default as well as custom ones created for the SonicWall Security Appliance.

- Address Objects
- Address Groups

From the **Address** page, you can perform the below operations:

- Filter the table data with possible combinations
- Add, modify, and delete custom objects and groups
- Clone from exiting objects and groups to create new objects and groups
- Purge to remove out-of-date ARP or DNS information
- Resolve DNS for the FQDN address objects
- Refresh and sort the table column data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

Topics:

- Default Address Objects and Groups
- Address Objects
- Address Groups
- Cloning Address Objects or Groups

Default Address Objects and Groups

Setting of the View drop-down menu to **Default** displays the default address objects and address groups of your firewall in the respective tabs.

Default address objects entries cannot be modified or deleted although some default address groups can be. Therefore, on the:

- **Address Objects** screen, the **Edit** and **Delete** icons are unavailable.
- **Address Groups** screen, the **Edit** icon for most entries and the **Delete** icon for all but a few entries are dimmed. Those entries that can be edited or deleted have the requisite icons available.

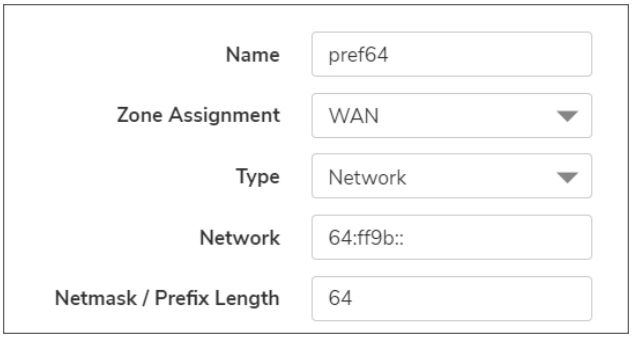
Topics:

- Default Pref64 Address Object
- Default Rogue Address Groups

Default Pref64 Address Object

SonicOS provides the default network address object, *Pref64* to support the NAT64 feature.

It is the original destination for a NAT64 policy and is always *pref64::/n*. You can create an address object of **Network** type to represent all addresses with *pref64::/n* to represent all IPv6 clients that can do NAT64. Refer to the below screen shot as an example.



A well-known prefix, *64:ff9b::/96*, is auto created by SonicOS. For more information about Pref64, refer to:

- NAT Rules section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
- NAT Policy section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

Default Rogue Address Groups

SonicOS provides the following default address groups for rogue wireless access points and devices.

- All Rogue Access Points
- All Rogue Devices

When Wireless Intrusion Detection and Prevention (WIDP) is enabled, SonicWave appliances act as both an access point and a sensor detecting any unauthorized access point connected to a SonicWall network.

WIDP automatically adds the detected:

- Rogue access points to the All Rogue Access Points address group
- Rogue devices to the All Rogue Devices address group

For more information about enabling options related to rogue access points, refer to the *Configuring Advanced IDP* in the *SonicOS Connectivity* administration documentation.

Address Objects

You can define the address objects and/or address groups one time and re-use them in multiple instances throughout the SonicOS interface.

Topics:

Types of Address Objects

Multiple address object types are available according to network address expressions as shown in the below table.

Type	Definition
Host	Defines a single host by its IP address and zone association. The netmask for a host address object is automatically set to 32-bit (*255.255.255.255*) to identify it as a single host. For example, *My Web Server* with an IP address of *67.115.118.110* and a default netmask of *255.255.255.255*.
Range	Defines a range of contiguous IP addresses. No netmask is associated with range address objects, but internal logic generally treats each member of the specified range as a 32-bit masked host object. For example, *My Public Servers* with an IP address starting value of *67.115.118.66* and an ending value of *67.115.118.90*. All 25 individual host addresses in this range are included in this address object.
Network	Similar to range objects in that they include multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network address objects must be defined by the network's address and a corresponding netmask. For example, *My Public Network* with a network address of *67.115.118.64* and a netmask of *255.255.255.224* would include addresses from *67.115.118.64* through *67.115.118.95*. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) cannot be assigned to a host.

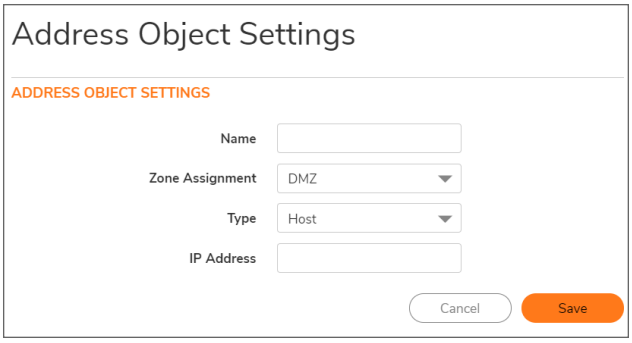
MAC	Allows for the identification of a host by its hardware address or IPv4/IPv6 MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6-byte hex-notation. For example, *My Access Point* with a MAC address of *00:06:01:AB:02:CD*. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance. MAC address objects are used by various components of wireless configurations throughout SonicOS, such as SonicPoint or SonicWave identification, and authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans. MAC address objects can also be used to allow hosts to bypass Guest Services authentication.
FQDN	Allows for the identification of a host by its IPv4/IPv6 Fully Qualified Domain Name (FQDN), such as *www.sonicwall.com*. FQDNs are be resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the responses to queries sent to the DNS servers.

Adding Address Objects

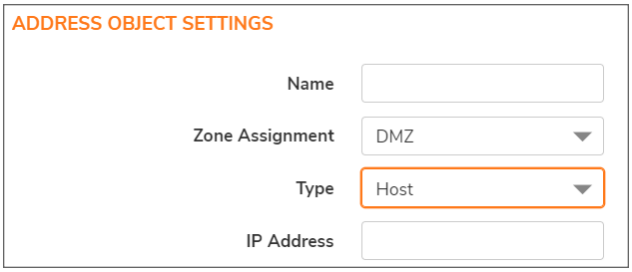
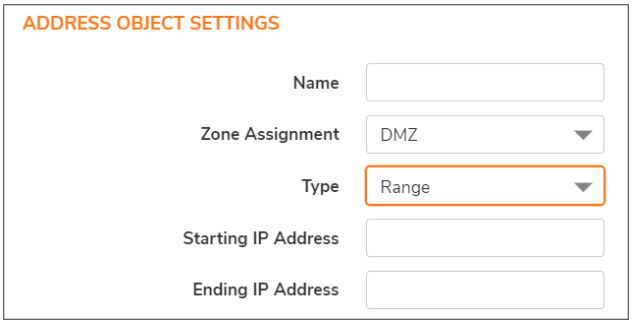
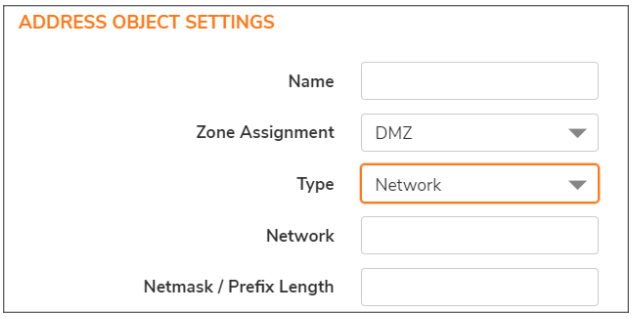
An address object must be defined before configuring NAT policies, access rules (Classic Mode) or security policies (Policy Mode, and services.

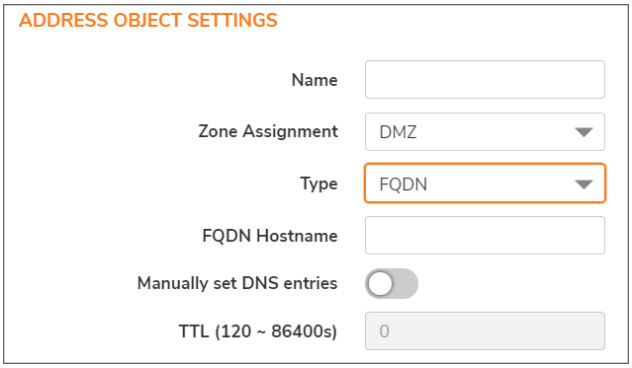
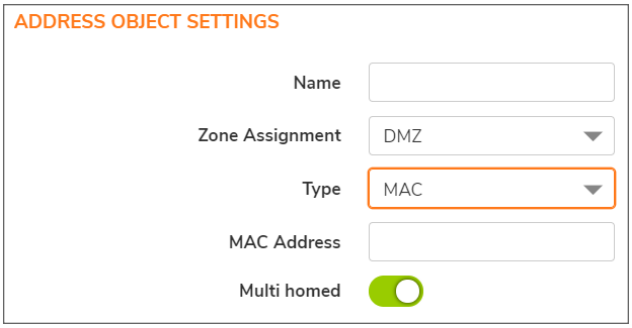
To add an address object:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Click the **Add** icon.



3. Enter a **Name** for the network address object.
4. Select a **Zone Assignment** for the address object.
5. Select one of the following **Type** from the drop-down menu and fill in the associated fields:

Address Object Type	Action with Associated Field	Screen Shot
Host	Enter an **IP Address**.	
Range	Enter **Starting IP Address** and **Ending IP Address**.	
Network	a. Enter the network IP address (such as 255.255.255.0) in the **Network** field. b. Enter the Netmask (such as 255.255.255.0) or prefix length (such as 24) in the **Netmask/Prefix Length** field.	

Address Object Type	Action with Associated Field	Screen Shot
FQDN	a. Enter the domain name for the individual site or range of sites (with a wildcard '*') in the **FQDN Hostname** field. b. Enable **Manually set DNS entries** to enter the time-to-live in seconds in the **TTL (120 ~ 86400s)** field if required. The minimum value is 120 and the maximum value is 86400 seconds.	
MAC	Enter the MAC address (such as 00:11:f5:1b:e3:cf) in the **MAC Address** field. By the default, **Multi homed** option is selected.	

6. Click **Save**.

Editing Address Objects

ⓘ | **NOTE:** You can edit all custom address objects and some of the default address objects.

To edit an address object:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Hover over the Address Object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Address Objects.
4. Click **OK**.

Deleting Custom Address Objects

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom address object or all custom address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Do one of the following:
   a. Hover over the custom address object to be deleted and click the **Delete** icon.
   b. Click the **Delete > Delete All** icon on top of the table to delete all custom address objects.
3. Click **OK**.

To delete multiple custom address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Select check boxes of the custom address objects to be deleted.
3. Click the **Delete > Delete Selected** icon on top of the table.
4. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Purging MAC or FQDN Address Objects

Purge is used to remove out-of-date ARP or DNS information from MAC or FQDN address objects.

To purge a MAC or FQDN address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Do one of the following:
   a. Select check boxes of the MAC or FQDN address objects and click the **Purge > Purge Selected** icon on top of the table to purge the selected custom address objects.
   b. Click the **Purge > Purge All** icon on top of the table to purge all MAC or FQDN custom address objects.

Resolving Address Objects

To resolve custom address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Select check boxes of the objects to be resolved.
3. Click the **Resolve > Resolve Selected** icon on top of the table.
   Selected objects get updated if any changes made to them.
4. Click **OK**.

To delete all custom address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
2. Click the **Resolve > Resolve All** icon on top of the table.
   All custom objects get updated if any changes made to them.

Address Groups

As more and more address objects are added to the firewall, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the address group are applied to each address in the group. Address groups can contain other address groups as well as address objects.

SonicOS has the ability to group the Address Objects and other Address Groups into Address Groups. Address Groups can be defined to introduce further referential efficiencies.

Address groups can contain any combination of host, range, or network address objects. For example, *My Public Group* can contain the host address object, *My Web Server*, and the range address object, *My Public Servers*, effectively representing IP addresses *67.115.118.66* to *67.115.118.90* and IP address *67.115.118.110*.

Dynamic address objects (MAC and FQDN) should be grouped separately, although they can safely be added to address groups of IP-based address objects, where they will be ignored when their reference is contextually irrelevant (for example, in a NAT policy).

Address groups are automatically created when certain features are enabled.

For example, in Classic Mode, a *Radius Pool* address group is created when the **Enable Local Radius Server** option is enabled on WLAN zone configuration, and are deleted when the feature is disabled. For more information, refer to Configuring the RADIUS Server.

Topics:

Adding Address Groups

To add an address group:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Groups**.
2. Click the **Add** icon.

3. Enter a **Name** for the network address group.
   Clear boxes of the address objects or groups to filter the required details in the **Not in Group** list.
   By the default, **All** box is selected. You can leave the **All** box selected to show all the address objects and groups in the **Not in Group** list.
4. Add address objects or groups to the address group in one of the following ways:
   - Select address objects or groups from the **Not in Group** list and click the right arrow.
     Press the **Ctrl** or **Shift** key to select multiple items.
   - Click the double right arrow to add all address objects and groups to the address group.
5. Remove address objects or groups from the address group in one of the following ways:
   - Select an item from the **In Group** list and click the left arrow to remove an item from the address group.
   - Click the double left arrow to remove all the address objects and groups from the address group.
6. Click **Save**.

Editing Address Groups

ⓘ | **NOTE:** You can edit all custom address groups and some of the default address groups.

To edit an address group:

1. Navigate to **OBJECT | Match Objects > Addresses**.
2. Click the **Address Groups** tab.
3. Hover over the address group to be edited and click the **Edit** icon.
4. Make the necessary changes to the address group.
   - Modify name of the address group
   - Add or remove address objects or groups
     For more information about adding or removing address objects or groups, refer to Adding Address Groups.
5. Click **Save**.

Deleting Custom Address Groups

ⓘ | **NOTE:**
- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

ⓘ | **NOTE:** You can delete only custom address groups.

To delete a custom address group or all custom address groups:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Groups**.
2. Do one of the following:
   a. Hover over the custom address group to be deleted and click the **Delete** icon.
   b. Click the **Delete > Delete All** icon on top of the table to delete all custom address groups.
3. Click **OK**.

To delete multiple custom address groups:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Groups**.
2. Select check boxes of the custom address groups to be deleted.
3. Click the **Delete > Delete Selected** icon on top of the table.

4. Do one of the following:
    a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
    b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Purging or Resolving All Address Groups

To purge or resolve all MAC or FQDN address objects:

1. Navigate to **OBJECT | Match Objects > Addresses > Address Groups**.
2. Click the **Purge All** or **Resolve All** icon on top of the table.
   All the groups get updated.

Cloning Address Objects or Groups

You can create a new item quickly from an existing item using clone operation.

ⓘ | **NOTE:** You can clone from all custom and the default items.

To clone from an existing object or group:

1. Navigate to **OBJECT | Match Objects > Addresses**.
2. Click **Address Objects** or **Address Groups** under which you want to create a new item.
3. Hover over the object or group from which you want to clone and click the **Clone** icon.
   This creates a duplicate of the item, which allows you to create a new one with the same settings.
4. Make the necessary changes.
5. Click **Save**.

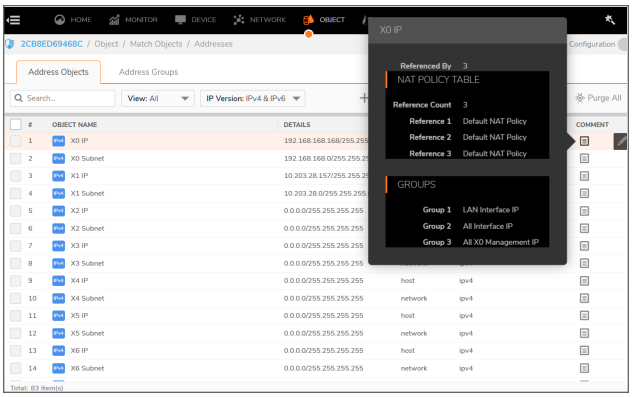
About UUIDs for Address Objects and Groups

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify address objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated, read-only internal value with these properties:

- A UUID is a unique representation of a SonicOS entity across the network.
- A UUID is generated at creation of an entity and removed at the deletion of the entity. It is not reused once it is removed.
- When an entity is modified, the UUID stays the same.
- UUIDs are regenerated after restarting the appliance with factory default settings.

By the default, UUIDs are not displayed in the Address Objects and Groups. You can customize the table to display UUIDs according to Common Actions with Objects Table.

When displayed, UUIDs appear in the tables for each object or group type.



UUIDs facilitate the following functions:

- You can search for an address object or group by UUID with the global search function of the management interface.
- You can view the reference count and referring entities if an object or group object with a UUID is referenced by another entity with a UUID. Hover over the **REFERENCES** column to view the reference count and referring entities.

Working with Dynamic Address Objects

From its inception, SonicOS has used address objects to represent IP addresses in most areas throughout the user interface. For more information, refer to Types of Address Objects.

SonicOS supports the following types of dynamic address objects:

Object Type	Description
MAC	SonicOS resolves MAC AOs to an IP address by referring to the ARP cache on the firewall.
FQDN	Fully Qualified Domain Names, such as *www.reallybadWebsite.com*, are resolved to their IP address (or IP addresses) using the DNS servers configured on the firewall. Wildcard entries using * are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Topics:

- Key Features of Dynamic Address Objects
- Enforcing the Use of Sanctioned Servers on the Network
- Using MAC and FQDN Dynamic Address Objects

Key Features of Dynamic Address Objects

The term *Dynamic Address Object (DAO)* describes the underlying framework enabling address objects (AOs) of MAC and FQDN. By transforming AOs from static to dynamic structures, access rules can automatically respond to changes in the network.

Below table provides details and examples for DAOs.

DYNAMIC ADDRESS OBJECTS: FEATURES AND BENEFITS

Feature	Benefit

FQDN wildcard support	FQDN address objects support wildcard entries, such as **.somedomainname.com*, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall.
	
	For example, creating an FQDN AO for **.myspace.com* will first use the DNS servers configured on the firewall to resolve *myspace.com* to *63.208.226.40*, *63.208.226.41*, *63.208.226.42*, and *63.208.226.43* (as can be confirmed by nslookup myspace.com or equivalent). As most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the firewall looks for DNS responses coming from sanctioned DNS servers as they traverse the firewall. So, if a host behind the firewall queries an external DNS server that is also a configured/defined DNS server on the firewall, the firewall parses the response to see if it matches the domain of any wildcard FQDN AOs.
	
	ⓘ
		NOTE:
		
		• Sanctioned DNS servers are those DNS servers configured for use by firewall. The reason is that responses from only sanctioned DNS servers are used in the wildcard learning process to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of access rules, as described in Enforcing the Use of Sanctioned Servers on the Network
		• For example:
		  • Assume the firewall is configured to use DNS servers *4.2.2.1* and *4.2.2.2*, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against *4.2.2.1* or *4.2.2.2* for *vids.myspace.com*, the response is examined by the firewall and matched to the defined **.myspace.com* FQDN AO. The result (*63.208.226.224*) is then added to the resolved values of the **.myspace.com* DAO.
		  • If the workstation, client-A, had resolved and cached *vids.myspace.com* before the creation of the **.myspace.com* AO, *vids.myspace.com* would not be resolved by the firewall because the client would use its resolver's cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about *vids.myspace.com* unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command **ipconfig / flushdns**. This forces the client to resolve all FQDNs, thereby allowing the firewall to learn them as they are accessed.
		• Wildcard FQDN entries resolve all hostnames within the context of the domain name, up to 256 entries per AO.
		  For example, **.sonicwall.com* resolves *www.sonicwall.com*, *software.sonicwall.com*, and *licensemanager.sonicwall.com*, to their respective IP addresses, but it does not resolve *sslvpn.demo.sonicwall.com* because it is in a different context; for *sslvpn.demo.sonicwall.com* to be resolved by a wildcard FQDN AO, the entry **.demo.sonicwall.com* would be required, which would also resolve *sonicos-*

Feature	Benefit
	enhanced.demo.sonicwall.com, *csm.demo.sonicwall.com*, *sonicos-standard.demo.sonicwall.com*, and so on. • Wildcards only support full matches, not partial matches. In other words, **.sonicwall.com* is a legitimate entry, but *w*.sonicwall.com*, **w.sonicwall.com*, and *w*w.sonicwall.com* are not. A wildcard can only be specified once per entry, so **.*.sonicwall.com*, for example, is not functional.
FQDN resolution using DNS	FQDN address objects are resolved using the DNS servers configured on the firewall in the **NETWORK | DNS** page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process retrieves all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
MAC address resolution using live ARP cache data	When a node is detected on any of the firewall's physical segments through the ARP (Address Resolution Protocol) mechanism, the firewall's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC address objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (for example, the host is no longer L2 connected to the firewall) the MAC AO will transition to an unresolved state.
MAC address object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the access rules, etc., that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the firewall's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create address groups of sanctioned servers (for example, SMTP, DNS)
- Create access rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

- Create access rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53).

  ⓘ **IMPORTANT:** Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.

- Create access rules in the relevant zones allowing firewalled hosts to only communicate via DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.
- Unsanctioned access attempts will then be viewable in the logs.

Using MAC and FQDN Dynamic Address Objects

Dynamic Address Objects (DAOs) of MAC and FQDN provide extensive access rule construction flexibility. DAOs of MAC and FQDN are configured in the same way as static address objects configured on the **OBJECT | Match Objects > Addresses > Address Objects** page. For more information, refer to Adding Address Objects. Once created, hover over the created address object to view the status. Log events record the addition and deletion of address objects.

Dynamic address objects lend themselves to many applications. The following are just a few examples of how they may be used.

Topics:

- Blocking All Protocol Access to a Domain using FQDN DAOs
- Using an Internal DNS Server for FQDN-based Access Rules or Security Policies
- Controlling a Dynamic Host's Network Access by MAC Address
- Bandwidth Managing Access to Entire Domain

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on trusted ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.

ⓘ **NOTE:** A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions:

- The firewall is configured to use DNS server *10.50.165.3, 10.50.128.53*.
- The firewall is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.

  ⓘ **NOTE:** DNS communications to unsanctioned DNS servers optionally can be blocked with access rules, as described in Enforcing the Use of Sanctioned Servers on the Network.
- The DSL home user is registering the hostname, moosifer.dyndns.org, with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.

  ⓘ **NOTE:** A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

To block all protocol access to a domain:

1. Create a FQDN address object according to Adding Address Objects.

   When first created, this entry will resolve only to the address for *dyndns.org*, for example, `63.208.196.110`. When a host behind the firewall attempts to resolve *moosifer.dyndns.org* using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.
2. Create an Access Rule or a Security Policy.
   - Classic Mode: An Access Rule on the **POLICY | Rules and Policies > Access Rules** page. For more information, refer to Configuring Access Rules section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
   - Policy Mode: A Security Policy on the **POLICY | Rules and Policies > Security Policy**. For more information, refer to Security Policy section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

Any protocol access to target hosts within that FQDN are blocked and the access attempt will be logged.

Using an Internal DNS Server for FQDN-based Access Rules or Security Policies

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft's DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server, refer to Microsoft Knowledge base article, How to configure *DNS dynamic updates in Windows*.

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymuth.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*.

```
 19 2.100829  10.50.165.249      2420  10.50.165.3        53    DNS    Dynamic update SOA moosifer.com
 20 2.105100  10.50.165.3        53    10.50.165.249      2420  DNS    Dynamic update response CNAME A 10.50.165.249

⊞ Frame 19 (122 bytes on wire, 122 bytes captured)
⊞ Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
⊞ Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
⊞ User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0bad
  ⊟ Flags: 0x2800 (Dynamic update)
      0... .... .... .... = Response: Message is a query
      .010 1... .... .... = Opcode: Dynamic update (5)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Zones: 1
    Prerequisites: 2
    Updates: 0
    Additional RRs: 0
  ⊟ Zone
    ⊟ moosifer.com: type SOA, class IN
        Name: moosifer.com
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  ⊟ Prerequisites
    ⊟ bohuymuth.moosifer.com: type CNAME, class NONE
        Name: bohuymuth.moosifer.com
        Type: CNAME (Canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
    ⊟ bohuymuth.moosifer.com: type A, class IN, addr 10.50.165.249
        Name: bohuymuth.moosifer.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 0 time
        Data length: 4
        Addr: 10.50.165.249
```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host's Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC address objects to control a host's access by its relatively immutable MAC (hardware) address.

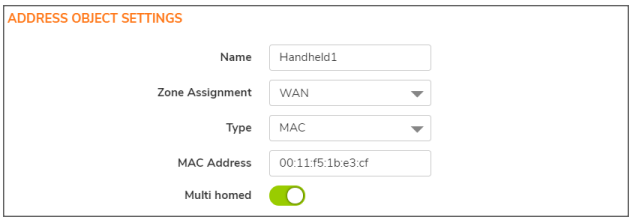
Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

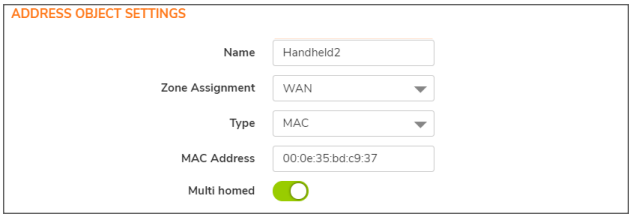
Example:

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (for example, 10.50.165.2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the 10.50.165.2 server, but to no other LAN resources. All other wireless clients should not be able to access the *10.50.165.2* server, but should have unrestricted access everywhere else.

To control a Dynamic Host's network access by MAC address for above example:

1. Create MAC Address Objects.
    a. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
    b. Click the **Add** icon and create the following MAC address objects (multi-homing is optional).





Once created, if the hosts are present in the firewall's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the **Address Objects** table until they are activated and are discovered through ARP.

c. Create an address group for the handheld devices according to Adding Address Groups.

2. Create an Access Rule or a Security Policy.

   Classic Mode: Create an access rule on the **POLICY | Rules and Policies > Access Rules** page. For more information, refer to **Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

   Policy Mode: Create a security policy on the **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

SAMPLE ACCESS RULES

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
Allow / Deny	Allow	Deny	Allow	Deny
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.2	10.50.165.2	Any	Any
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on

ⓘ **NOTE:** The MediaMoose Services service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

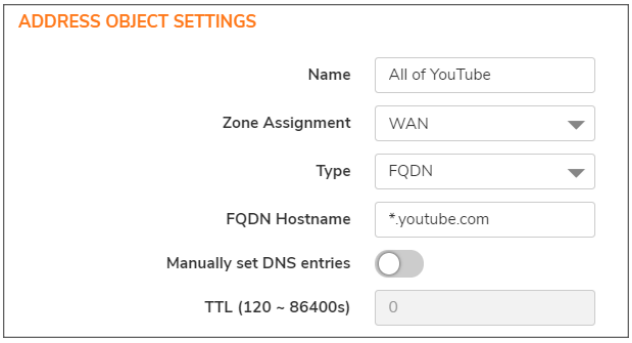
Bandwidth Managing Access to Entire Domain

ⓘ | **NOTE:** This section is applicable only for Classic Mode.

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN address objects can be used to simplify this effort. Below is an example of controlling access to entire domain by bandwidth management.

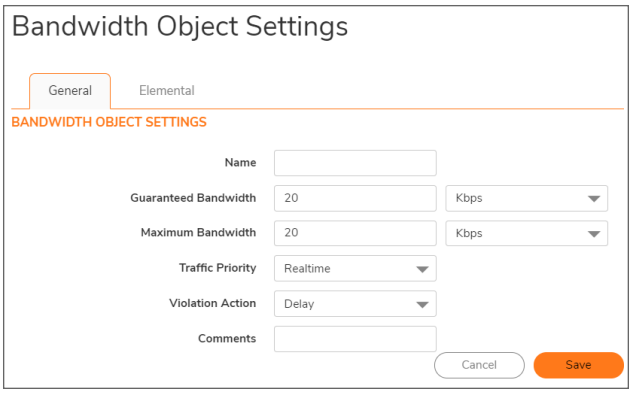
To control access to entire domain by bandwidth management:

1. Create FQDN Address Objects..
   a. Navigate to **OBJECT | Match Objects > Addresses > Address Objects**.
   b. Click **Add** and create the following address object.

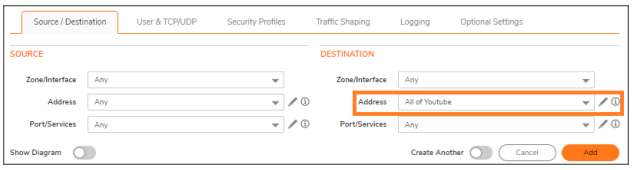


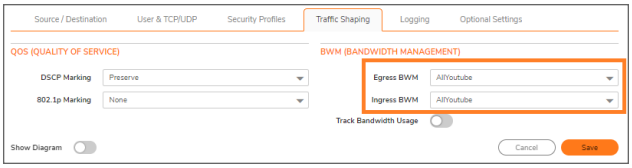
   Upon initial creation, **.youtube.com* resolves to IP addresses *208.65.153.240*, *208.65.153.241*, *208.65.153.242*, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries are added, such as the entry for the *v87.youtube.com* server (*208.65.154.84*).

2. Create the Bandwidth Object.
   a. Navigate to **OBJECT | Profile Objects > Bandwidth**.
   b. Click **Add** and create the bandwidth object.



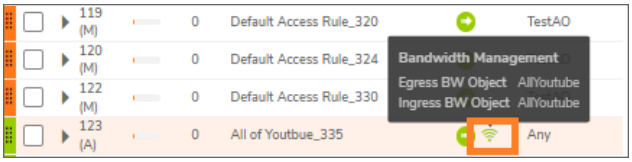
3. Create an Access Rule.
   a. Navigate to **POLICY | Rules and Policies | Access Rules**.
   b. Click **Add** and create the Access Rule with Address Object and Bandwidth profile object created in the above steps.





For more information, refer to SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

After the access rule is created, the Bandwidth Management icon appears within the Access Rule table, indicating that BWM is active and providing statistics. Hover over the icon to see the BWM settings.



Access to all *.youtube.com hosts, using any protocol, is now be cumulatively limited to speed that you have set, a low percentage of your total available bandwidth for all user sessions.

3

Services

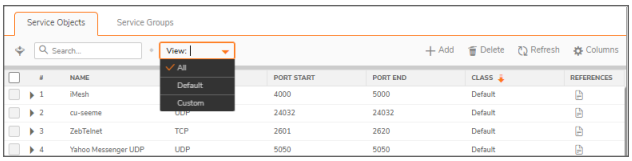
SonicOS supports an expanded IP protocol to allow users to create service objects, service groups, and access rules (Classic Mode) or security policies (Policy Mode based on these custom service protocols.

For more information about:

- A list of default protocols, refer to Default IP Protocols for Custom Service Objects.
- Adding specific IP protocols required for your network, refer to Adding Custom IP Protocol Services.

Services are used by the SonicWall security appliance to configure access rules or security policies for allowing or denying traffic to the network. The SonicWall security appliance includes default service objects and default service groups. You can edit, but not delete, default service objects and default service groups. You can create custom service objects and custom service groups to meet your specific business requirements.

The **View** drop-down menu at the top of the page allows you to control the display of default and custom service objects and groups. Select **All** type to display both custom and default entries, select **Custom** to display only custom or select **Default** to display only default service entries.



Topics:

- Default Service Objects and Groups
- Default IP Protocols for Custom Service Objects
- Service Objects
- Service Groups
- Adding Custom IP Protocol Services

Default Service Objects and Groups

Default service objects and groups are predefined in SonicOS. You cannot delete the default service objects and groups, but you can edit:

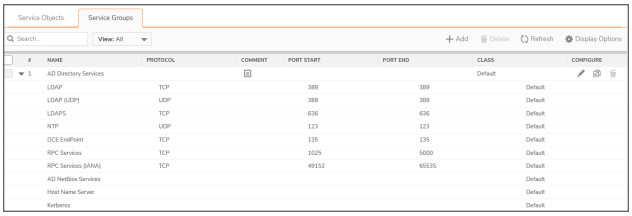
Default Type	Editable
Service object	To update ports only
Service group	To included or excluded services

Attributes of the **Service Objects** and **Service Groups** are shown in the below table.

Name	The name of the service
Protocol	The protocol of the service
Port Start	The starting port number for the service
Port End	The ending port number for the service
Class	Indicates if the entry is a **Default** (system) or **Custom** (user) service
References	Hover over the icon under the References column to display information about the service object or group. A pop-up displays the following: • **Referenced By** With a list of the types of rules or policies configured on the firewall which use the service object or group, along with the number of references to it for each type. The rule or policy type is displayed as a link when available, such as for **Access Rules**, **NAT Policies**, etc. You can click the link to go to the page to see the list of specific rules or policies using the service object or group. • **Groups (Member of)** With a list of service groups or other types of groups that include the service object or group.

Default service groups are groups of default service objects and/or other default service groups. Clicking on the triangle to the left of the group name displays all the individual default service objects and groups included in the group. For example, the **AD Directory Services** default group contains several service objects and service groups as shown in AD Directory Services group details image. By grouping these multiple entries together, they can be referenced as a single service in rules and policies throughout SonicOS.

AD DIRECTORY SERVICES GROUP DETAILS



Default IP Protocols for Custom Service Objects

Protocol	IP Number	Full Form	Description
ICMP	1	Internet Control Message Protocol	A TCP/IP protocol used to send error and control messages.
IGMP	2	Internet Group Management Protocol	The protocol that governs the management of multicast groups in a TCP/IP network.
TCP	6	Transmission Control Protocol	The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
UDP	17	User Datagram Protocol	A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
6over4	41	Transmission of IPv6 over IPv4 domains without explicit tunnels	The 6over4 traffic is transmitted inside IPv4 packets whose IP headers have the IP protocol number set to 41.
GRE	47	Generic Routing Encapsulation	A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Inter network.
ESP	50	Encapsulated Security Payload	A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
AH	51	Authentication Header	A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
ICMPv6/ND	58	Neighbor Discovery for Internet Message Control Protocol version 6	Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect message.

Protocol	IP Number	Full Form	Description
EIGRP	88	Enhanced Interior Gateway Routing Protocol	Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
OSPF	89	Open Shortest Path First	A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.

Protocol	IP Number	Full Form	Description
PIM	103	Protocol Independent Multicast	One of two PIM operational modes: • **PIM sparse mode (PIM-SM)** tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. • **PM dense mode (PIM-DM)** assumes all downstream routers and hosts want to receive a multicast datagram from a sender and floods multicast traffic throughout the network. Routers without downstream neighbors prune unwanted traffic. To minimize repeated flooding of datagrams and subsequent pruning, PIM DM uses a state refresh message sent by routers directly connected to the source. ⓘ **NOTE:** The firewall can be configured only as a multicast proxy so multicast traffic can be passed through the up / down stream interface. The firewall cannot act as a PIM router.
L2TP	115	Layer 2 Tunneling Protocol	A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Service Objects

You can add a custom service object for any of the default protocols or service types listed in Default IP Protocols for Custom Service Objects.

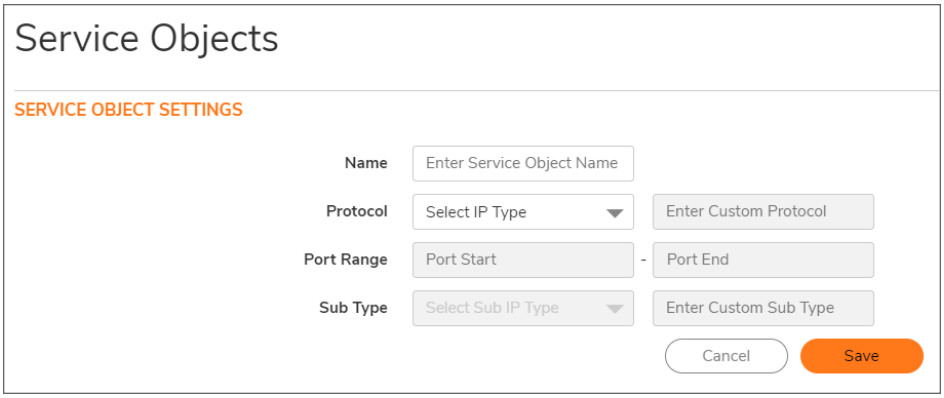
All custom service objects you create are listed in the **Service Objects** table. You can group custom services by creating a custom service group for easy policy enforcement. If a protocol is not listed as a default service object, you can add a custom service object for it.

Topics:

Adding Service Objects using Default Protocols

To add a custom service object using default protocols:

1. Navigate to **OBJECT | Match Objects > Services > Service Objects**.
2. Click the **Add** icon.



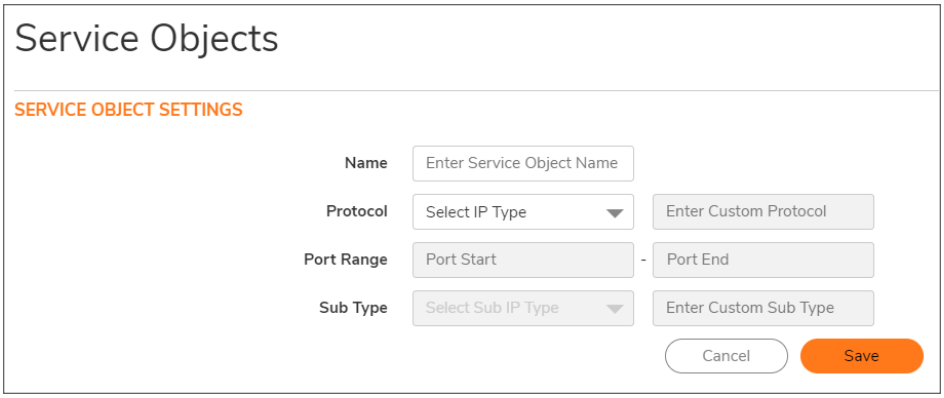
3. Enter a descriptive and unique **Name** for the service object.
4. Select type of IP **Protocol** and specify the details.
   - For **TCP** and **UDP** protocols, specify **Port Range**.
   - For **ICMP**, **IGMP**, **OSPF**, and **PIM** protocols, select a **Sub Type**.

     ⓘ **NOTE:** PIM subtypes apply to both PIM-SM and PIM-DM except the following are for PIM SM only:
     - Type1: Register
     - Type2: Register Stop
     - Type4: Bootstrap
     - Type8: Candidate RP Advertisement
     - For the remaining protocols, you do not need to specify anything further.

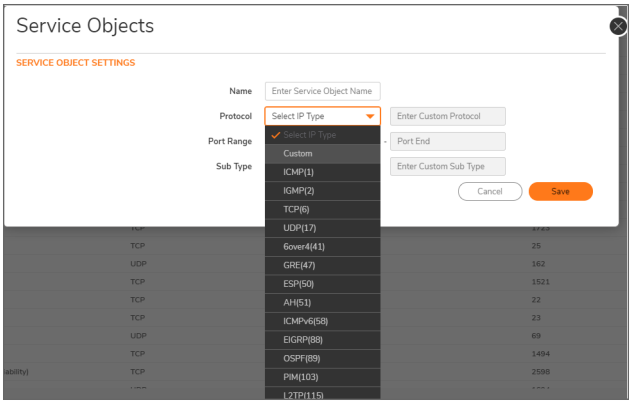
Adding Service Objects using Custom Protocols

To add a custom service object using custom protocols:

1. Navigate to **OBJECT | Match Objects > Services > Service Objects**.
2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the service object.
2. Select **Custom** IP type from the **Protocol** drop-down menu.



3. Enter custom protocol number for the **Custom** IP Type.

   NOTE:
   - **Enter Custom Protocol** number.
   - The **Port Range** and **Sub Type** fields are not applicable to a Custom IP Type.
   - Attempts to define a custom protocol type service object for a default IP type is not permitted and results in an error message.
4. Click **Save**.
5. Repeat the above steps for each custom service to be defined.

Editing Service Objects

ⓘ | **NOTE:** You can edit all custom service objects and some of the default service objects.

To edit a service object:

1. Navigate to **OBJECT | Match Objects > Services > Service Objects**.
2. Hover over the custom service object to be edited and click the **Edit** icon.
3. Make the necessary changes.

   ⓘ | **NOTE:** You cannot change name of the default objects.

   For more information, refer to Adding Service Objects using Default Protocols or Adding Service Objects using Custom Protocols.
4. Click **Save**.

Deleting Custom Service Objects

ⓘ | **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom service object:

1. Navigate to **OBJECT | Match Objects > Services > Service Objects**.
2. Set the **View** drop-down menu to **Custom**.
3. Hover over the object to be deleted and click the **Delete** icon.
4. Click **Confirm** in the confirmation dialog box.

To delete multiple or all custom service objects:

1. Navigate to **OBJECT | Match Objects > Services > Service Objects**.
2. Set the **View** drop-down menu to **Custom**.
3. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.

     All custom items get selected.

4. Do one of the following:
    a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
    b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Service Groups

You can add custom services and create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a custom service group.

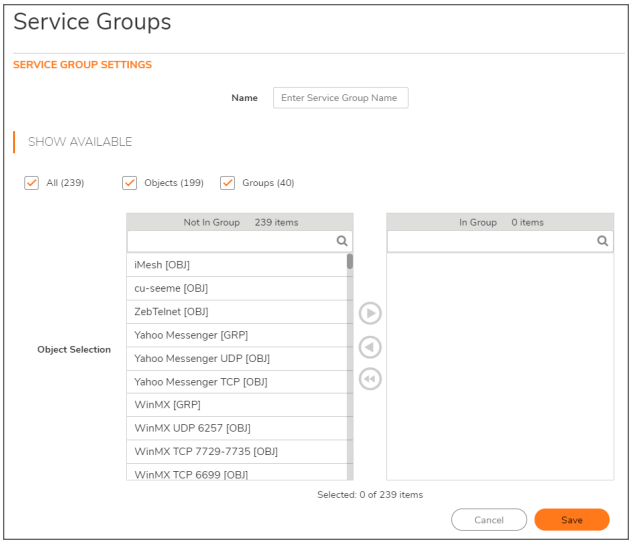
Topics:

- Adding Custom Service Groups
- Editing Service Groups
- Deleting Custom Service Groups

Adding Custom Service Groups

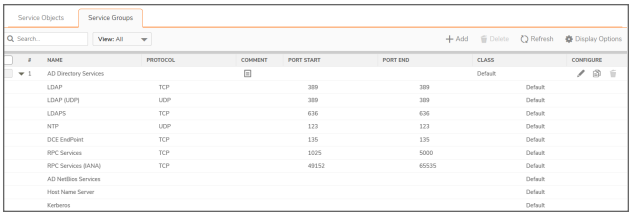
To add a custom service group:

1. Navigate to **OBJECT | Match Objects > Services > Service Groups**.
2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.

4. Select the objects or groups from the **Not in Group** list and click the right arrow to add them to the group. Press the **Ctrl** or **Shift** key to select multiple items.
5. Remove objects or groups from the group in one of the following ways:
    - Select an item from the **In Group** list and click the left arrow to remove the selected item from the group.
    - Click the left double arrow to remove all the items from the group.
6. Click **Save**.
7. Click the triangle available to the left side of the group **Name** to view all the individual custom services, default services, and custom services groups included in the custom service group.



Editing Service Groups

You also can edit individual services of a custom service group by expanding the group, and clicking the **Edit** icon for the service.

ⓘ | **NOTE:** You can edit all custom service groups and some of the default service groups.

To edit a custom service group:

1. Navigate to **OBJECT | Match Objects > Services > Service Groups**.
2. Hover over the service group to be edited and click the **Edit** icon.
3. Make the necessary changes.
    - Modify name of the group.
    - Add or remove address objects.
      For more information, refer to Adding Custom Service Groups.
4. Click **Save**.

Deleting Custom Service Groups

ⓘ | **NOTE:**
- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.

- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom service group:

1. Navigate to **OBJECT | Match Objects > Services > Service Groups**.
2. Set the **View** drop-down menu to **Custom**.
3. Hover over the object to be deleted and click the **Delete** icon.
4. Click **Confirm** in the confirmation dialog box.

To delete multiple or all custom service groups:

1. Navigate to **OBJECT | Match Objects > Services > Service Groups**.
2. Set the **View** drop-down menu to **Custom**.
3. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
4. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Adding Custom IP Protocol Services

Using only the default IP protocol types, if the security appliance encounters traffic of any other IP protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP protocols, as governed by IANA (Internet Assigned Numbers Authority), so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it is functionally restrictive.

SonicOS allows you to construct service objects representing any IP type, allowing access rules or security policies to then be written to recognize and control IP traffic of any type.

ⓘ **NOTE:** The generic service **Any** does not handle custom IP type service objects. In other words, simply defining a custom IP type service object for *IP Type 126* does not allow IP Type 126 traffic to pass through the default **LAN > WAN** Allow rule. You need to create an access rule or a security policy specifically containing the custom IP type service object to provide for its recognition and handling as described in Configuration Example.

Configuration Example

Assume an administrator needs to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, *10.50.165.26*). You can define custom IP type service objects to handle these two services.

To define a custom IP type service and related configuration:

1. Add custom service objects according to Adding Service Objects using Custom Protocols.

   Enter the protocol numbers as 46 and 119.

2. Add a service group named *myServices* according to Adding Custom Service Groups.

   Select the custom service objects created in step 1 from **Not in Group** list and click right arrow to add to the service group.

3. Add an address object for **Host** type and **WLAN** zone according to Adding Address Objects that the WLAN Subnets can access using *myServices*.

   Enter the Host IP address as *10.50.165.26*.

4. Define a **WLAN > LAN** access rule or security policy with **Source / Destination** attributes listed in the below table.

   - Classic Mode: An Access Rule on the **POLICY | Rules and Policies > Access Rules** page. For more information, refer to Configuring Access Rules section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
   - Policy Mode: A Security Policy on the **POLICY | Rules and Policies > Security Policy**. For more information, refer to Security Policy section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

Attribute	Source	Destination
Zone/Interface	WLAN	LAN
Address	WLAN Subnets	Host address object created in step 3
Port/Services	Any	*myServices* service group created in step 2

ⓘ **NOTE:** It may be necessary to create an access rule or security policy for bi-directional traffic. For example, an additional access rule or security policy from the **LAN > WLAN** allowing *myServices* from *10.50.165.26* to WLAN Subnets.

Now the traffic from IP protocols 46 and 119 is recognized and allowed to pass from WLAN Subnets to the host at *10.50.165.26*.

4

URI Lists

A **URI List Object** defines a list of URIs (Uniform Resource Identifiers) or domains that can be marked as allowed or forbidden. You can also export a URI list to an external file or import a file into a URI list.

ⓘ | **NOTE:** When processing, URI lists have a higher priority than the category of a URI.

URI List Objects have the following requirements:

- Up to 128 URI List Objects are allowed.
- Each URI List Object supports up to 5000 URIs. The minimum number is 1.
- Up to 100 Keywords can be configured in each URI List Object. The minimum is zero.

From the **URI Lists** page, you can:

- Search for the objects or groups with a specific string
- Add, modify, and delete website objects and groups
- Clone from an exiting group to create a new group
- Refresh and sort the table columns data to identify the specific results

Topics:

About URIs and the URI List

Each **URI List Object** must have at least one URI in its **URI List**. You can manually add entries to the **URI List** by typing or pasting them in or importing a list of URIs from a text (*.txt*) file. The file can be a manually created one or a file that was previously exported from the appliance. Each URI in the file is on its own line.

You can export the **URI List** contents into a text file that you can import later.

The URIs and **URI List** have the following requirements:

- Each URI can be up to 255 characters.
- The maximum combined length of all URIs in one URI List is 131,072 (1024*128) characters, including one character for each new line (carriage return) between the URIs.
- By definition, a URI is a string containing host and path. Port and other content are currently not supported, but you can use Keywords to match these.
- The host portion of a URI can be an IPv4 or IPv6 address string.
- Each URI can contain up to 16 tokens. A token in a URI is a string composed of the characters:

  0 through 9
  a through z
  A through Z
  $ - _ + ! ' ( ) , .

  - Each token can be up to 64 characters, including one character for each separator (. or /) surrounding the token.
  - An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens, not one or more characters.

Examples of valid URIs	Examples of invalid URIs
• *news.example.com* • *news.example.com/path* • *news.example.com/path/abc.txt* • *news.*.com/*.txt* • *10.10.10.10* • *10.10.10.10/path* • *[2001:2002::2003]/path* • *[2001:2002::2003:*:2004]/path/*.txt*	Using the wildcard character (*) incorrectly can result in invalid URIs such as: • *example*.com* • *exa*ple.com* • *example.*.*.com* ⓘ **NOTE:** The wildcard character represents a sequence of one or more tokens, not one or more characters.

About Keywords and the Keyword List

A URI List Object uses its URI List to match URIs when scanning web traffic. It uses a token-based match algorithm, which means torrent.com does not match seedtorrent.com. The Keyword List makes URI matching more flexible, allowing the URI List Object to match traffic by matching other portions of a URI.

If a web traffic URI string (host+path+queryString) has any sub-string in the keyword list, the URI List Object gets a match. For example, if *sports* and *news* are in the keywords list, the URI List Object can match www.extremsports.com, news.google.com/news/headlines?ned=us&hl=en, or www.yahoo.com/?q=sports.

As with the URI List, you can manually add entries to the **Keyword List** by typing or pasting them in, or importing a list of keywords from a text (*.txt*) file. The file can be a manually created one or a file that was previously exported from the appliance. Each URI in the file is on its own line.

You can export the **Keyword List** contents into a text file that you can import later.

Keyword and Keyword List have the following requirements:

- Each keyword can contain up to 255 printable ASCII characters.
- The maximum combined length of keywords in one **Keyword List** is limited to 1024 * 2, including one character for each new line (carriage return) between the keywords.

Matching URI List Objects

The matching process for **URI List Objects** is based on tokens. A valid token sequence is composed of one or more tokens, joined by a specific character, like dot (.) or forward slash (/). A URI represents a token sequence. For example, the URI *www.example.com* is a token sequence consisting of www, example, and com, joined by a dot (.). Generally, the URI List Object matches that URI if a URI contains one of the URIs in a URI List Object.

Topics:

- Normal Matching
- Wildcard Matching
- IPv6 Address Matching
- IPv6 Wildcard Matching

Normal Matching

If a list object contains a URI such as *example.com*, then that object matches URIs defined as:

[<token sequence>(.|/)]example.com[(.|/)<token sequence>]

For example, the URI List Object matches any of the following URIs:

- *example.com*
- *www.example.com*
- *example.com.uk*
- *www.example.com.uk*
- *example.com/path*

The URI List Object does not match the URI, *specialexample.com*, because *specialexample* is identified as a different token than *example*.

Wildcard Matching

Wildcard matching is supported. An asterisk (*) is used as the wildcard character and represents a valid sequence of tokens. If a list object contains a URI such as *example.*.com*, then that list object matches URIs defined as:

[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]

For example, the URI List Object *example.*.com* matches any of the following URIs:

- *example.exam1.com*
- *example.exam1.exam2.com*
- *www.example.exam1.com/path*

The URI List Object does not match the URI:

- *example.com*

This is because the wildcard character (*) represents a valid token sequence that isn't present in *example.com*.

IPv6 Address Matching

IPv6 address string matching is also supported. While an IPv4 address can be handled as a normal token sequence, an IPv6 address string needs to be handled specially. If a URI List Object contains a URI such as *[2001:2002::2008]*, then that URI List Object matches URIs defined as:

[2001:2002::2008][/<token sequence>]

For example, the URI List Object matches any of the following URIs:

- *[2001:2002::2008]*
- *[2001:2002::2008]/path*
- *[2001:2002::2008]/path/abc.txt*

IPv6 Wildcard Matching

Wildcard matching in the IPv6 address string is supported. If a list object contains a URI such as *[2001:2002:*:2008]/*/abc.mp3*, then that list object matches URIs defined as:

[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3

For example, the URI List Object matches any of the following URIs:

- *[2001:2002:2003::2007:2008]/path/abc.txt*
- *[2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt*

Using URI List Objects

Currently, URI List Objects can be used in these fields:

- Allowed URI List of a CFS profile
- Forbidden URI List of a CFS profile
- Web Excluded Domains of Websense

CFS URI List Objects are used in these fields differently. When used in an Allowed or URI Forbidden List of a CFS profile, the CFS URI List Object acts normally. For example, if the URI List Object contains a URI such as *example.com/path/abc.txt*, then that list object matches URIs defined as:

[<token sequence>(.|/)] example.com/path/abc.txt[(.|/)<token sequence>]

When used by the Web Excluded Domains of Websense, only the host portion of the URI takes effect. For example, if the URI List Object contains the same URI as above, *example.com/path/abc.txt*, then that list object matches all domains containing the token sequence *example.com*. The path portion in the URI is ignored.

About URI List Groups

Starting from SonicOS 6.5.2, URI List Groups are supported for flexible and convenient management of URI List Objects, including CFS profile allowed and forbidden lists or for a Websense exclusion list. You can assign multiple URI List Objects to one group and refer to that group directly within other modules. The URI List Group supports nested inclusion, allowing one URI List Group to contain other URI List Groups. A URI List Group can be used anywhere that a URI List Object can be used.

You can configure up to 128 URI List Groups and the maximum length of a URI List Group name is 49 characters. You can assign up to 128 URI List Objects and/or URI List Groups to a URI List Group. The maximum number of unique URIs is 5000 and the maximum number of unique keywords is 100.

Managing URI List Objects

Topics:

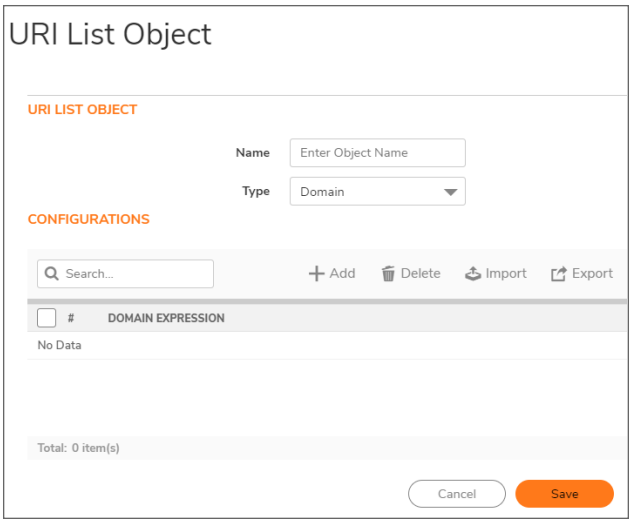
About the URI List Objects Table

Name	Name of the URI List Object.
URI List	Specifies the URIs in the URI List Object.
Type	Specifies the URI typeconfigured in the URI List Object.
Group Reference Count	Specifies the URI group objects.

Adding URI List Objects

To add URI List Objects:

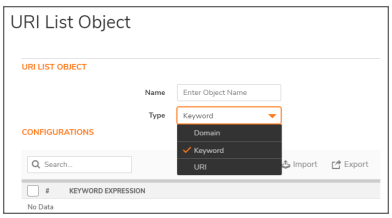
1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the URI List Object.
4. Add URIs in one of the following ways:
   You can either add or import the URIs from a text (.txt) file.
   - Add the URIs manually
   - Import the URIs from a text file
5. Add the Keywords if you wish to add in one of the following ways:
   - Add the Keywords manually
   - Import the Keywords from a text file
6. Click **Save**.

Adding URIs

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Click the **Add** icon.
3. Set the **Type** as URI.



4. Click the **Add** icon.
5. Enter a URI and click **OK**.
   ⓘ | **NOTE:** For more information about URI requirements, refer to About URIs and the URI List.
6. Repeat the process until all the URIs are added to the list.
7. Click **Save**.

Importing URIs

Importing URIs from a file, overwrites the URIs which were added manually.

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Click the **Add** icon.
3. Set the **Type** as URI on the **URI List Object** dialog box.
4. Click the **Import** icon and select the text file.
   ⓘ | **IMPORTANT:** Make sure that the text file is conformed to the conditions stated in About URIs and the URI List.

URIs in the text file can be separated by any of the separators listed below by pressing **Enter** or **Return** on keyboard:

Separator	Style
\r\n	Windows style, new line separator
\r	MAC OS style, new line separator
\n	UNIX style, new line separator

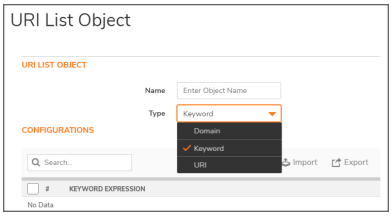
Only the first 2000 valid URIs in the file are imported. Invalid URIs are skipped and do not count toward the maximum of 2000 URIs per **URI List Object**.

5. Click **Confirm** in the pop-up window.
6. Select the file and click **Open**.

   Populates the URI List Object table with URIs imported from the text file. Any URIs that were added manually are replaced by the URIs in the imported file.

Adding Keywords

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Click the **Add** icon.
3. Set the **Type** as Keyword.



4. Click the **Add** icon.
5. Enter a Keyword and click **OK**.

   NOTE: For more information about keywords and the **Keyword List**, refer to About Keywords and the Keyword List.

6. Repeat the process until all the keywords are added to the list.
7. Click **Save**.

Importing Keywords

Importing Keywords from a file, overwrites the Keywords which were added manually.

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Click the **Add** icon.
3. Set the **Type** as Keyword on the **URI List Object** dialog box.
4. Click the **Import** icon.

5. Click **Confirm** in the pop-up window.

   NOTE: For more information about keywords and the **Keyword List**, refer to About Keywords and the Keyword List.

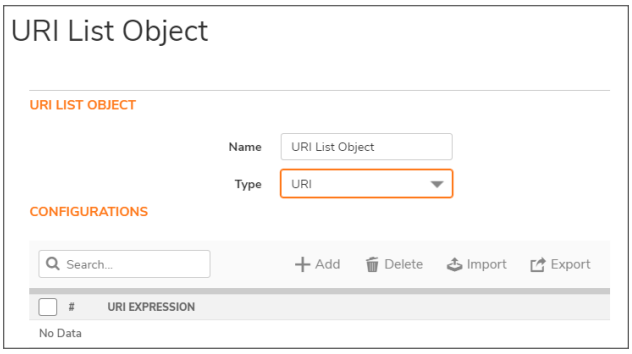
6. Select the file and click **Open**.

   Populates the URI List Object table with keywords imported from the text file. Any keywords that were added manually are replaced by the keywords in the imported file.

Exporting URI List Objects

To export URI List Object:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Hover over the list object from the list and click the **Edit** icon.



3. Click the **Export** icon.

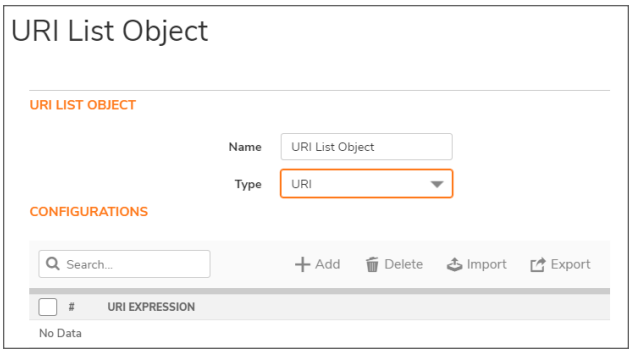
   All the items available in the URI List Object are exported and downloaded as a text (.txt) file.

4. Click **Cancel** in the **URI List Object** dialog box.

Editing URI List Objects

To edit a URI List Object:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Hover over the URI list object to be edited and click the **Edit** icon.



3. Remove the URI List Object entries in one of the following ways:
   - Hover over the URI List Object and click the **Delete** icon.
   - Select check boxes of the URI List Objects and click the **Delete** icon on top of the table. Click **Confirm**.
4. Add or import the URI List Object entries.
   - Add the URIs manually or Import the URIs from a text file
   - Add the Keywords manually or Import the Keywords from a text file
5. Click **Save**.

Deleting URI List Objects

ⓘ | **NOTE:** You cannot delete an object if it is in use by CFS Profile.

To delete a URI List Object:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple URI List Objects:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Objects**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table. All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.

b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Managing URI List Groups

Topics:

About the URI List Groups Table

Name	Name of the URI List Group.
URI List	Specifies the URIs in the URI List Group.
Type	Specifies the URI type configured in the URI List Group.
Policy Reference Count	Specifies the group policy.

Adding URI List Groups

To add a URI List Group:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Groups**.
2. Click the **Add** icon.
3. Enter a descriptive and unique **Name** for the group.
4. Select the objects or groups from the **Not in Group** list and click the right arrow to add them to the group. Press the **Ctrl** or **Shift** key to select multiple items.
5. Remove objects or groups from the group in one of the following ways:
   - Select an item from the **In Group** list and click the left arrow to remove the selected item from the group.
   - Click the left double arrow to remove all the items from the group.
6. Click **Save**.

Editing a URI List Group

To edit a URI List Group:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Groups**.
2. Hover over the group to be edited and click the **Edit** icon.
3. Make the necessary changes.
   - Modify name of the group
   - Add or remove objects or groups
     For more information about adding or removing URI List objects or groups, refer to Adding URI List Groups.
4. Click **Save**.

Deleting URI List Groups

ⓘ | **NOTE:** You cannot delete a group if it is in use by CFS Profile.

To delete a URI List Group:

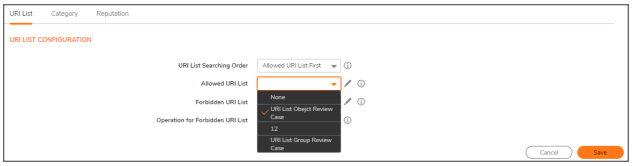
1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Groups**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all URI List Objects:

1. Navigate to **OBJECT | Match Objects > URL Lists > URI List Groups**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying URI List Object or Group

You can apply these URI list objects or groups to set allowed or forbidden URI list in Adding CFS Profile Objects on **OBJECT | Profile Objects > Content Filter** page.



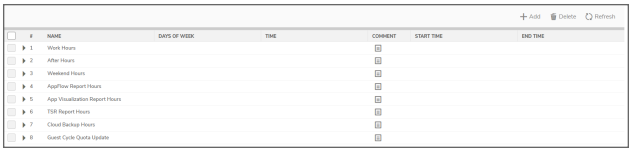
5

Schedules

SonicOS uses schedule objects in conjunction with its security features and policies. You can apply schedule objects for a specific access rule (Classic Mode) or security policy (Policy Mode). Default and custom schedule objects help to enforce schedule times for a variety of SonicWall Security Appliance features.

A schedule can include multiple days and time increments for rule enforcement with a single schedule.

The **Schedules** page displays the Default Schedules and custom schedules if any.



From **Schedules** page, you can:

- Filter the table data for **Used and Unused** schedules
- Add, delete custom schedules
- Modify default and custom schedules
- Clone from an exiting one to create a new one
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- View the list of policies where the schedule is used.

Topics:

Default Schedules

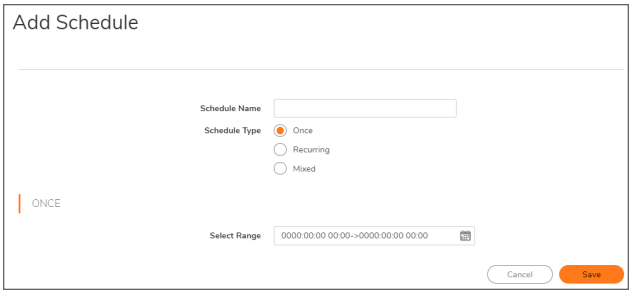
The **Schedules** table displays all default and custom schedules. The default schedules consist of:

Work Hours	After Hours
Weekend Hours	AppFlow Report Hours
App Visualization Report Hours	TSR Report Hours
Cloud Backup Hours	Guest Cycle Quota Update

Adding Custom Schedules

To create custom schedules:

1. Navigate to **OBJECT | Match Objects > Schedules**.
2. Click the **Add** icon.



3. Enter a **Rule Name**.
4. Select the option for **Schedule Type**:

Once	For one-time schedule between the configured **Start** and **End** times and dates. When selected, the fields under **Once** become available, and the fields under **Recurring** become dimmed.
Recurring	For a schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become available, and the fields under **Once** become dimmed.
Mixed	For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.

ⓘ | **NOTE:** Time must be in 24-hour format, for example, 17:00 for 5 p.m.

5. Add schedule based on the **Schedule Type** selection.

Schedule Type	Procedure
Once	1. Enter **Start Time** and **Stop Time**. ⓘ | **NOTE:** Time must be in 24-hour format, for example, 17:00 for 5 p.m. 2. Click **Add**. 3. Repeat the process to include multiple schedules to the same rule.
Recurring	1. Do one of the following: • Enable a day or multiple days of the week in **Select Day** list to create a rule for any specific days. • Enable **Select All** to create a rule for entire week. 2. Enter **Start Time** and **Stop Time**. ⓘ | **NOTE:** Time must be in 24-hour format, for example, 17:00 for 5 p.m. 3. Click **Add**. 4. Repeat the process to include multiple schedules to the same rule.

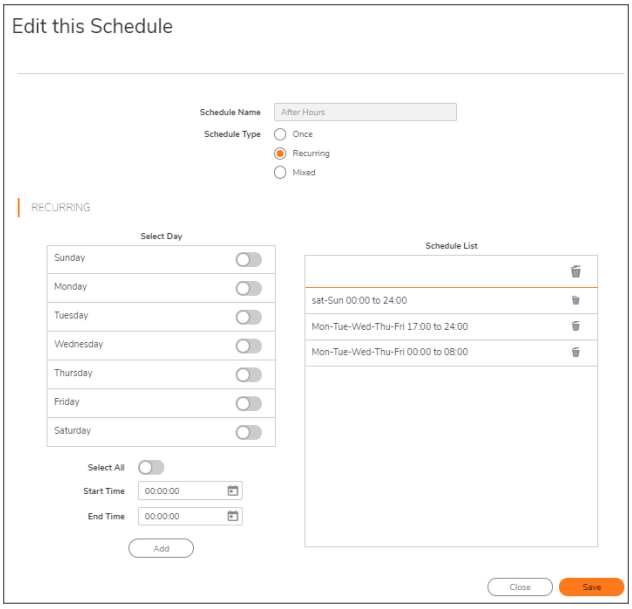
6. Add schedule details according to the above step if **Schedule Type** is selected as **Mixed**.
   You can mix both types of schedules, **Once** and **Recurring** for **Mixed** type.
7. Click **Save**.
   The **Schedule** is created.

Editing Schedules

ⓘ | **NOTE:** You can edit the default schedules also.

To edit a schedule:

1. Navigate to **OBJECT | Match Objects > Schedules**.
2. Hover over the schedule to be edited and click the **Edit** icon.



3. Make the necessary changes.
   - Modify **Schedule Name** and **Schedule Type**.
     ⓘ | **NOTE:** You cannot change the **Schedule Name** for the default schedules.
   - Delete the existing schedules from the list if **Schedule Type** is **Recurring** or **Mixed**.
   - Add new schedules to the list if **Schedule Type** is **Recurring** or **Mixed**.

   For more information, refer to Adding Custom Schedules.
4. Click **Save**.

Deleting Custom Schedules

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom schedule object:

1. Navigate to **OBJECT | Match Objects > Schedules**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all custom schedule objects:

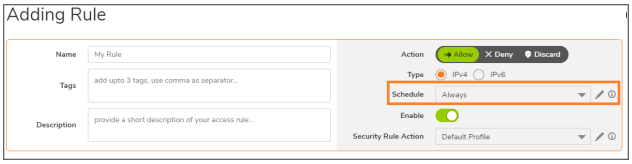
1. Navigate to **OBJECT | Match Objects > Schedules**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Schedules

You can apply the default or custom schedule objects in defining:

- Classic Mode: An Access Rule on the **POLICY | Rules and Policies > Access Rules** page. For more information, refer to **Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

- Policy Mode: A Security Policy on the **POLICY | Rules and Policies > Security Policy**. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



6

Dynamic Group

Dynamic Groups are comprised of Dynamic External Address Groups (DEAG) and Dynamic External Address Objects (DEAO). A DEAG is an Address Group whose members are dynamic. DEAOs are intermediate, internal objects that are dynamically created and placed under a DEAG when a DEAG file is downloaded. The Dynamic External Objects feature eliminates the need for manually modifying an Address Group to add or remove members.

DYNAMIC GROUP PAGE

Pop-up tool tips appear when you hover over many of the fields in a DEAG entry.

You can configure multiple Dynamic External Address Groups which can be used in access rules or security policies.

For example, if you want to maintain a group for all partner IP addresses on which certain access rules or security policies are enforced, you can create a DEAG or DEAO.

The creation of a DEAO consists:

- Creation of the DEAG file on an FTP server or on a web page at a specific URL
- Configuration of the DEAG on the **OBJECT | Match Objects > Dynamic Group** page including downloading and using the information in the DEAG file.

From **Dynamic Group** page, you can:

- Filter the table data with a specific string
- Add, modify, and delete Dynamic External Address Groups
- Export the table information into CSV file
- Refresh the table to get the latest data

Topics:

About Dynamic External Address Group File

The Dynamic External Address Group (DEAG) file contains a list of IP addresses or Fully Qualified Domain Names (FQDNs) that define the DEAOs which are members of the DEAG. The DEAG file resides externally, on a server for FTP access or on a web page at a specific URL for HTTPS access. The list of IP addresses or FQDNs can be modified at the external location and the associated DEAOs and DEAG in SonicOS are dynamically updated with those changes, if configured to periodically download the file.

The DEAG file can contain a text list of either IP addresses or FQDNs formatted as follows:

- A list of IP addresses, one per line. It can include subnets specified in CIDR format.
- A list of FQDNs, one per line. An FQDN is a character string such as **www.example.com**. It cannot contain any wildcard (*) characters.
- A mixed list of FQDNs and IP addresses/subnets, one per line. This is only supported for FQDN type DEAGs. A non-FQDN type DEAG will not accept FQDNs in the DEAG file.

  However, it is not recommended to mix and match IP addresses and FQDNs in the DEAG file, because the IP addresses in this list will also be treated as FQDNs and SonicOS attempts to resolve them. A better way to mix these input types is to create individual DEAGs of FQDN type and non-FQDN type and then add both DEAGs to a separate address group for use in access rules or security policies.

For every DEAG, a DEAO with the IP address *0.0.0.0* is automatically created. For example, if there is only one DEAG, the maximum number of IP addresses in the DEAG file is one less than the maximum number of DEAOs allowed, as defined in DEAG and DEAO Maximums.

DEAG and DEAO Maximums

Maximum DEAGs:

- The maximum number of DEAGs, including both IP address and FQDN types, is 25% of the total number of address groups supported by the device.
- The maximum number of DEAGs that can be created cannot exceed the number of address groups remaining before exceeding the total number supported on the firewall.

  For example, if a device supports 1024 Address Groups and you are using only 20 Address Groups, then 256 DEAGs (25% of 1024) can be created. However, if you have already manually created 1000 Address Groups, then only 24 DEAGs can be created.

Maximum DEAOs:

- The maximum number of *IP address type* DEAOs is 25% of the total number of address objects supported by the device.
- The maximum number of *FQDN* type DEAOs is 50% of the total number of address objects supported by the device.
- The maximum number of DEAOs that can be created cannot exceed the number of address objects remaining before exceeding the total number supported on the firewall.

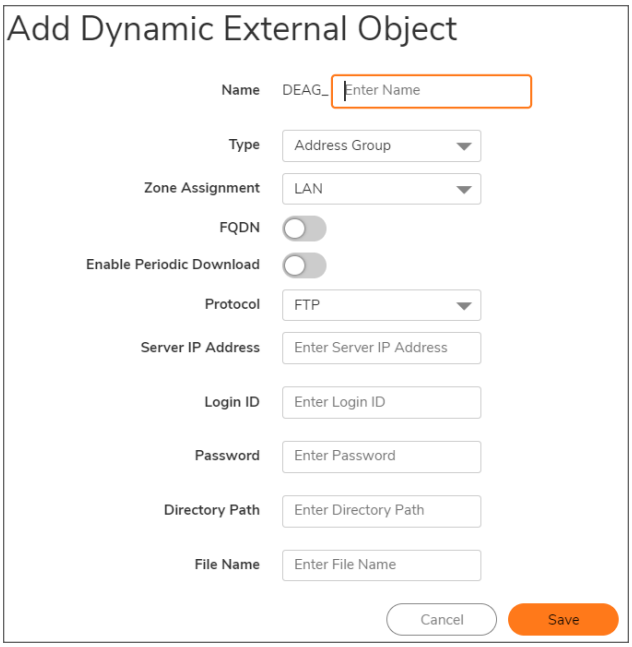
High Availability Requirements

When deployed as a High Availability pair, both the active and standby firewalls must have a connection to the server or URL to download the file that contains the list of IP addresses or FQDNs. This requires configuring the monitoring IP address on the standby unit.

Adding Dynamic External Objects

To add a Dynamic External Object:

1. Navigate to **OBJECT | Match Objects > Dynamic Group**.
2. Click the **Add** icon.



3. Enter a **Name** for the dynamic external address group.

   NOTE:
   - **DEAG_** is automatically prepended to the name when saved.
   - Only alphabets and numerical values without spaces are allowed in the **Name** field.
   - **Type** is set to *Address Group*, with no other options.
4. Select the **Zone Assignment** for the Dynamic External Address Group.
5. **Enable FQDN** to create a Dynamic External Address Group of type FQDN.

   Enable FQDN only when you want to create an Address Group that contains multiple Address objects of FQDN type. All the Address Objects need to be of type FQDN.
6. **Enable Periodic Download** for ongoing, periodic downloads of the Dynamic Address Group File.
   - Select the number of minutes or hours between downloads in the Download Interval field. You can select one of:
     - 5 minutes
     - 15 minutes

- 1 hour
- 24 hours

7. Select the **protocol** to be used for downloading the DEAG file.

Protocol	Specification	Description
FTP	Server IP Address	IP address of the FTP server where the DEAG file resides. For more information, refer to About Dynamic External Address Group File.
	Login ID	User name for logging into the FTP server
	Password	Password for logging into the FTP server
	Directory Path	Folder in which the DEAG file resides on the FTP server
	File Name	Name of the DEAG file on the FTP server
HTTPS	URL Name	URL which has the list of IP addresses or FQDNs. The URL Name should start with *https://* and follow with the page name.

8. Click **Save**.

Based on the configuration, the firewall reads the list of IP addresses or FQDNs from the file or URL and SonicOS automatically creates read-only address group and address objects which cannot be edited or deleted:

- Address group with the name provided in the **Add Dynamic External Object** dialog box.
- Address objects for every valid unique IP address or FQDN in the file.

The individual address objects are added to the Dynamic External Address Group or Dynamic External Object. You can use this group or object in access rules (Classic Mode) or security policies (Policy Mode).

Editing Dynamic External Objects

To edit a dynamic external object:

1. Navigate to **OBJECT | Match Objects > Dynamic Group**.
2. Click the **Edit** icon in the **Configure** column of the Dynamic External Object to be edited.
3. Make the necessary changes. For more information, refer to Adding Dynamic External Objects.
   You cannot change the **Name** of the DEAG and the **Zone Assignment**.
4. Click **Save**.

Deleting Dynamic External Objects

ⓘ | **NOTE:** You cannot delete an object if it is in use by Rule.

To delete a Dynamic External Object:

1. Navigate to **OBJECT | Match Objects > Dynamic Group** page.
2. Click the **Delete** icon in the **Configure** column for the object to be deleted.
3. Click **Confirm**.

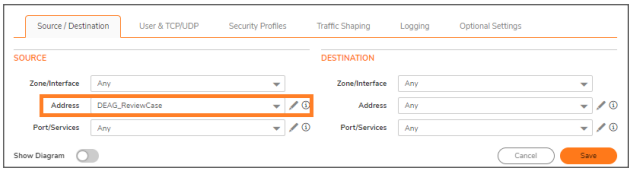
To delete multiple Dynamic External Objects:

1. Navigate to **OBJECT | Match Objects > Dynamic Group** page.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

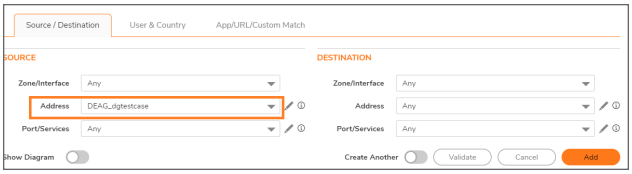
Applying Dynamic External Objects

Once the Dynamic Group are created, you can apply them in defining:

- Classic Mode: An Access Rule on the **POLICY | Rules and Policies > Access Rules** page. For more information, refer to **Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.



- Policy Mode: A Security Policy on the **POLICY | Rules and Policies > Security Policy**. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



7

Email Addresses

Application control allows the creation of custom email address lists as email address objects. Email address objects can represent individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an App Rules policy or a Security Policy of type SMTP client. For more information, refer to Applying Email Addresses Objects.

From **Email Addresses** page, you can:

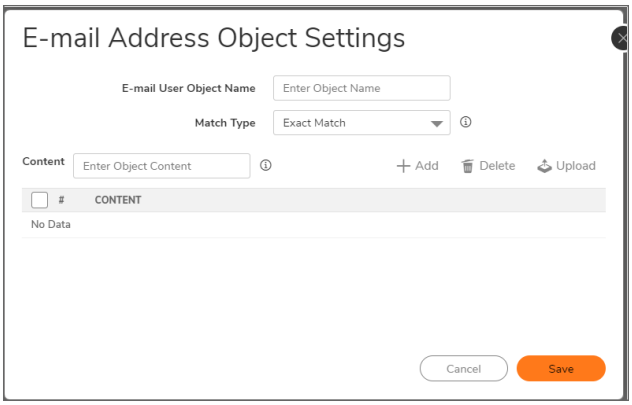
- Filter the table data with a specific string
- Add, modify, and delete objects
- Refresh and sort the table columns data to identify the specific results

Topics:

Adding Email Address Objects

To configure an email address object:

1. Navigate to **OBJECT | Match Objects > Email Addresses**.
2. Click the **Add** icon.



3. Enter an **Email User Object Name**.
4. Select a **Match Type**.

Exact Match	To exactly match the email address that you provide.
Partial Match	To match any part of the email address.
Regex Match	To use a regular expression to match the email address.

5. Add the object **Content** in one of the following ways:
   - Enter an email id to match in the **Content** field and click the **Add** icon.

     You can add multiple entries to create a list of **Content** elements to match.

     Examples:
     - To match on a domain, select Match Type as **Partial Match** and enter **@** followed by the domain name in the **Content** field, for example, **@sonicwall.com**.
     - To match on an individual user, select Match Type as **Exact Match** and enter the full email address in the **Content** field, for example, **jsmith@sonicwall.com**.
   - Click **Upload** icon and import a list of elements from a text file.

     Make sure that each element in the file must be on a line by itself.

   Multiple entries, either from a text file or entered manually, are displayed in the List. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.
6. Click **Save**.

   New object is created and listed on the **OBJECT | Match Objects > Email Address** page.

Editing Email Address Objects

To edit an email address object :

1. Navigate to **OBJECT | Match Objects > Email Addresses**.
2. Hover over the object to be edited and click the **Edit** icon.
3. Add or Delete the email addresses to the object.
   For more information, refer to Adding Email Address Objects.
4. Click **Add**.

Deleting Email Address Objects

ⓘ | **NOTE:** You cannot delete an object if it is in use by Rule.

To delete an email address object :

1. Navigate to **OBJECT | Match Objects > Email Addresses**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all address objects:

1. Navigate to **OBJECT | Match Objects > Email Addresses**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Email Addresses Objects

You can only use email address objects with App Rules policies (in Classic Mode) or Security Policies (in Policy Mode) when the **Policy Type** is **SMTP Client**.

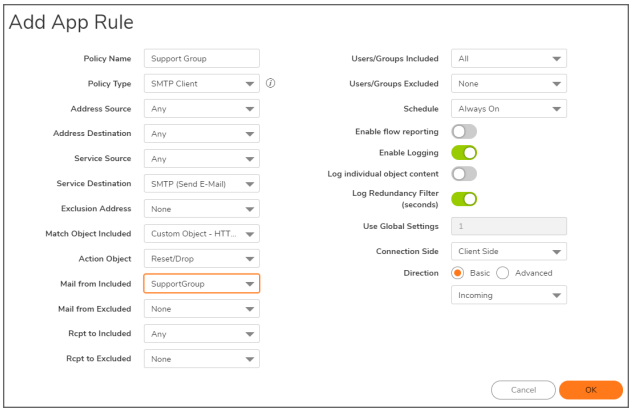
Here is an example to understand how an email address object works. Considered creating an SMTP client policy that includes or excludes the group.

In Classic Mode:

1. Create an email address object to represent the **support group**. For more information, refer to Adding Email Address Objects.
2. Create an App Rule on the **POLICY | Rules and Policies > App Rules** page. For more information, refer to Configuring App Rules section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

   Exclude the support group from a policy that prevents executable files from being attached to outgoing email.

   You can use the email address object in **Mail from Included**, **Mail from Excluded**, **RCPT to Included**, or **RCPT to Excluded** of the SMTP client policy. The **Mail from** refer to the sender of the email. The **RCPT to** refer to the intended recipient.



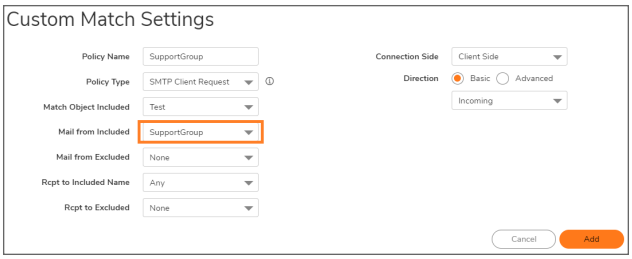
   Although App Rules cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. While creating an email address object for this group, import the list from the text file. For more information, refer to Adding Email Address Objects.

In Policy Mode:

1. Create an email address object to represent the **support group**. For more information, refer to Adding Email Address Objects.
2. Create a custom match object with email address object created in the above step. For more information about creating a custom match object, refer to Custom Match Objects.

Exclude the support group from a policy that prevents executable files from being attached to outgoing email.

You can use the email address object in **Mail from Included**, **Mail from Excluded**, **RCPT to Included**, or **RCPT to Excluded** of the SMTP client policy. The **Mail from** refer to the sender of the email. The **RCPT to** refer to the intended recipient.



3. Create a custom match group with the custom match object created in the above step. For more information about creating a custom match group, refer to Custom Match Groups.
4. Configure a Security Policy with the custom match object created in the above step. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

   Although security policies cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. While creating an email address object for this group, import the list from the text file. For more information, refer to Adding Email Address Objects.

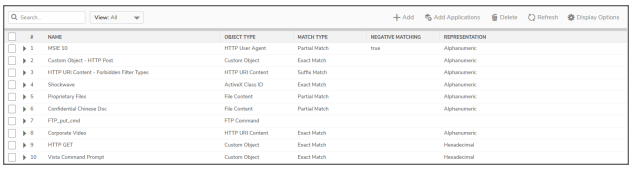
8

Match Objects

The **Match Objects** feature is available only in Classic Mode.

From the **Match Objects** page, you can:

- Search for the match objects or application list objects with a specific string
- Add, modify, and delete match objects or application list objects
- Clone from an exiting object to create a new object
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

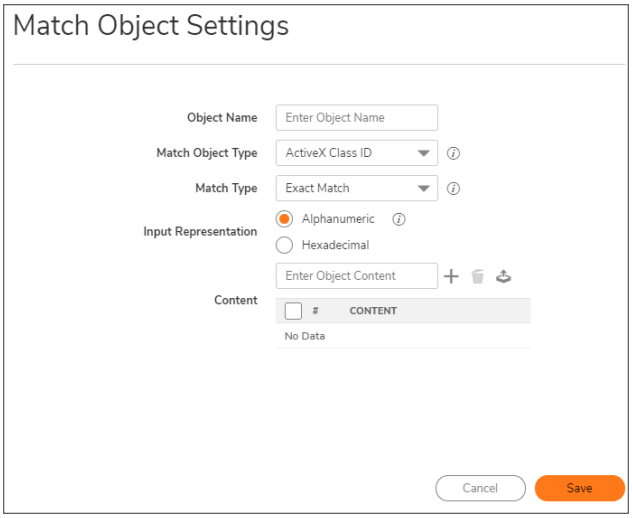


Topics:

Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. Match objects include:

- Match Object Type. For more information, refer to Supported Match Object Types.
- Match Type (exact, partial, regex, prefix, or suffix). For more information, refer to Supported Match Object Types.
- Input representation.
- Actual content to match. The File Content match object type provides a way to match a pattern or keyword within a file.



ⓘ | **NOTE:** Match objects were referred to as application objects in previous releases.

Topics:

- Input representation
- Supported Match Object Types
- Regular Expressions
- Negative Matching
- Adding Match Objects
- Editing Match Objects

Input representation

Representation	Used to match	Example
Hexadecimal	Binary content Hexadecimal representation can be used for binary content found in a graphic image.	Executable files
Alphanumeric (text)	Things Alphanumeric (text) can be used to match the same graphic if it contains a certain string in one of its properties fields.	File or email content
Regular expressions (regex)	A pattern rather than a specific string or value Regular expressions (regex) use Alphanumeric input representation.	For more information, refer to Regular Expressions.

Supported Match Object Types

The below table describes the supported match object types and associated match types.

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is **c1fb8842-5281-45ce-a271-8fd5f117ba5**f	Exact	No	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
Custom Object	Allows specification of an IPS-style custom set of conditions	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email	Partial	No	None
Email CC	Any content in the CC MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email From	Any content in the From MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent	N/A	No	None
Email Subject	Any content in the Subject MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email To	Any content in the To MIME Header	Exact, Partial, Prefix, Suffix	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed. Provides a way to match a pattern or keyword within a file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.	Partial	No	**Disable attachment** action should never be applied to this object.
File Extension	**For** / **Extension of** Email / An attachment HTTP / An uploaded attachment to the Web mail account FTP / An uploaded or downloaded file	Exact	Yes	None
File Name	**For** / **File Name of** Email / An attachment HTTP / An uploaded attachment to the Web mail account FTP / An uploaded or downloaded file	Exact, Partial, Prefix, Suffix	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
FTP Command	Allows selection of specific FTP commands	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Cookie	Allows specification of a Cookie sent by a browser	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Host	Content found inside of the HTTP Host header. Represents host name of the destination server in the HTTP request, such as *www.google.com*.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Referrer	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Set Cookie	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Prefix, Suffix	No	None
HTTP URL	Any HTTP URL that needs to be matched.	Exact, Partial, Prefix, Suffix	No	None
HTTP User Agent	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None
IPS Signature Category List	Available only in Classic Mode. Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures.	N/A	No	None
IPS Signature List	Available only in Classic Mode. Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None
Application Category List	Available only in Classic Mode. Allows specification of application categories, such as Multimedia, P2P, or Social Networking	N/A	No	None

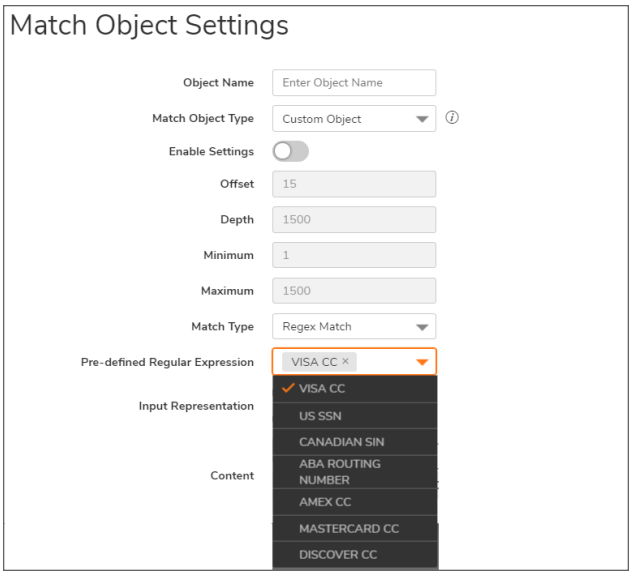
Object Type	Description	Match Types	Negative Matching	Extra Properties
Application List	Available only in Classic Mode. Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Available only in Classic Mode. Allows specification of individual signatures for the application and category that you select	N/A	No	None
Log Email User	Log SMTP E-mail users	N/A	No	None

Regular Expressions

You can configure regular expressions in certain types of match objects for use in App Rules policies. The Match Object Settings options provide a way to configure custom regular expressions or to select from predefined regular expressions. The SonicWall implementation supports reassembly-free regular expression matching on network traffic. This means that no buffering of the input stream is required and patterns are matched across packet boundaries.

SonicOS provides the following predefined regular expressions:

VISA CC	VISA Credit Card Number
US SSN	United States Social Security Number
CANADIAN SIN	Canadian Social Insurance Number
ABA ROUTING NUMBER	American Bankers Association Routing Number
AMEX CC	American Express Credit Card Number
MASTERCARD CC	Mastercard Credit Card Number
DISCOVER CC	Discover Credit Card Number



Policies using regular expressions match the first occurrence of the pattern in network traffic. This enables actions on matches as soon as possible. Because matching is performed on network traffic and not only on human-readable text, the matchable alphabet includes the entire ASCII character set — all 256 characters.

Popular regular expression primitives such as '.', (any character wildcard), '*', '?', '+', repetition count, alternation, and negation are supported. Though the syntax and semantics are similar to popular regular expression implementations such as Perl, vim, and others, there are some minor differences. For example, beginning (^) and end of line ($) operators are not supported. Also, '\z' refers to the set of non-zero digits, [1-9], not to the end of the string as in PERL. For more information about syntax, refer to Regular Expression Syntax.

One notable difference with the Perl regular expression engine is the lack of back-reference and substitution support. These features are actually extraneous to regular expressions and cannot be accomplished in linear time with respect to the data being examined. Hence, to maintain peak performance, they are not supported. Substitution or translation functionality is not supported because network traffic is only inspected, not modified.

Predefined regular expressions for frequently used patterns such as U.S. social security numbers and VISA credit card numbers can be selected while creating the match object. Users can also write their own expressions in the same match object. Such user provided expressions are parsed and any that do not parse correctly will cause a syntax error to display at the bottom of the Match Object Settings window. After successful parsing, the regular expression is passed to a compiler to create the data structures necessary for scanning network traffic in real time.

Regular expressions are matched efficiently by building a data structure called *Deterministic Finite Automaton* (DFA). The DFA's size is dictated by the regular expression provided by the user and is constrained by the memory capacities of the device. A lengthy compilation process for a complex regular expression can consume extensive amounts of memory on the appliance. It may also take up to two minutes to build the DFA, depending on the expressions involved.

To prevent abuse and denial-of-service attacks, along with excessive impact to appliance management responsiveness, the compiler can abort the process and reject regular expressions that cause this data structure to grow too big for the device. An **abuse encountered** error message is displayed at the bottom of the window.

NOTE: During a lengthy compilation, the appliance management session may become temporarily unresponsive, while network traffic continues to pass through the appliance.

Building the DFA for expressions containing large counters consumes more time and memory. Such expressions are more likely to be rejected than those that use indefinite counters such as the '*' and '+' operators.

Also, at risk of rejection are expressions containing a large number of characters rather than a character range or class. That is, the expression '(a|b|c|d|. . .|z)' to specify the set of all lower-case letters is more likely to be rejected than the equivalent character class '\l'. When a range such as '[a-z]' is used, it is converted internally to '\l'. However, a range such as '[d-y]' or '[0-Z]' cannot be converted to any character class, is long, and may cause the rejection of the expression containing this fragment.

Whenever an expression is rejected, the user may rewrite it in a more efficient manner to avoid rejection using some of the above tips. For more information about syntax, refer to Regular Expression Syntax. For an example on how to write a custom regular expression, refer to **Creating a Regular Expression in a Match Object** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

Regular Expression Syntax

This section provides the information about syntax that are used in building regular expressions.

REGULAR EXPRESSION SYNTAX: SINGLE CHARACTERS

Representation	Definition
.	Any character except **\n**. Use **/s** (stream mode, also known as single-line mode) modifier to match **\n** too.
[xyz]	Character class. Can also give escaped characters. Special characters do not need to be escaped as they do not have special meaning within brackets [ ].
\xdd	Hex input. **dd** is the hexadecimal value for the character. Two digits are mandatory. For example, **\r** is **\x0d** and not **\xd**.
[a-z][0-9]	Character range.

REGULAR EXPRESSION SYNTAX: COMPOSITES

Representation	Definition
xy	x followed by y
x|y	x or y
(x)	Equivalent to x. Can be used to override precedences.

REGULAR EXPRESSION SYNTAX: REPETITIONS

Representation	Definition
x*	Zero or more x
x?	Zero or one x
x+	One or more x

Representation	Definition
x{n, m}	Minimum of **n** and a maximum of **m** sequential x's. All numbered repetitions are expanded. So, making m unreasonably large is ill-advised.
x{n}	Exactly n x's
x{n,}	Minimum of n x's
x{,n}	Maximum of n x's

REGULAR EXPRESSION SYNTAX: ESCAPE SEQUENCES

Representation	Definition
\0, \a, \b, \f, \t, \n, \r, \v	**C** programming language escape sequences (**\0** is the NULL character (ASCII character zero)).
\x	Hex-input. **\x** followed by two hexa-decimal digits denotes the hexa-decimal value for the intended character.
***, \?, \+, \(, \), \[, \], \{, \}, \\, \/, \<space>, \#**	Escape any special character. ⓘ **NOTE:** Comments that are not processed are preceded by any number of spaces and a pound sign (#). So, to match a space or a pound sign (#), you must use the escape sequences **** and **\#**.

REGULAR EXPRESSION SYNTAX: PERL-LIKE CHARACTER CLASSES

Representation	Definition
\d, \D	Digits, Non-digits.
\z, \Z	Non-zero digits ([1-9]), All other characters.
\s, \S	White space, Non-white space. Equivalent to [\t\n\f\r]. \v is not included in Perl white spaces.
\w, \W	Word characters, Non-word characters Equivalent to [0-9A-Za-z_].

REGULAR EXPRESSION SYNTAX: OTHER ASCII CHARACTER CLASS PRIMITIVES

If you want...	...then use	
[:cntrl:]	\c, \C	Control character. [\x00 - \x1F\x7F].
[:digit:]	\d, \D	Digits, Non-Digits. Same as Perl character class.
[:graph:]	\g, \G	Any printable character except space.
[:xdigit:]	\h, \H	Any hexadecimal digit. [a-fA-F0-9]. Note this is different from the Perl \h, which means a horizontal space.
[:lower:]	\l, \L	Any lower case character.
[:ascii:]	\p, \P	Positive, Negative ASCII characters. [0x00 – 0x7F], [0x80 – 0xFF].
[:upper:]	\u, \U	Any upper case character.

Some of the other popular character classes can be built from the above primitives. The following classes do not have their own short-hand due of the lack of a nice mnemonic for any of the remaining characters used for them.

REGULAR EXPRESSION SYNTAX: COMPOUND CHARACTER CLASSES

If you want...	... then use	
[:alnum:]	= [\l\u\d]	The set of all characters and digits.
[:alpha:]	= [\l\u]	The set of all characters.
[:blank:]	= [\t<space>]	The class of blank characters: tab and space.
[:print:]	= [\g<space>]	The class of all printable characters: all graphical characters including space.
[:punct:]	= [^\P\c<space>\d\u\l]	The class of all punctuation characters: no negative ASCII characters, no control characters, no space, no digits, no upper or lower characters.
[:space:]	= [\s\v]	All white space characters. Includes Perl white space and the vertical tab character.

REGULAR EXPRESSION SYNTAX: MODIFIERS

Representation	Definition
/i	Case-insensitive
/s	Treat input as single-line. Can also be thought of as stream-mode. That is, dot (**.**) matches **\n** too.

REGULAR EXPRESSION SYNTAX: OPERATORS IN DECREASING ORDER OF PRECEDENCE

Operators	Associativity
[ ], [^]	Left to right
()	Left to right
***, +, ?**	Left to right
. (Concatenation)	Left to right
|	Left to right

Comments in Regular Expressions

SonicOS supports comments in regular expressions. Comments are preceded by any number of spaces and a pound sign (#). All text after a space and pound sign is discarded until the end of the expression.

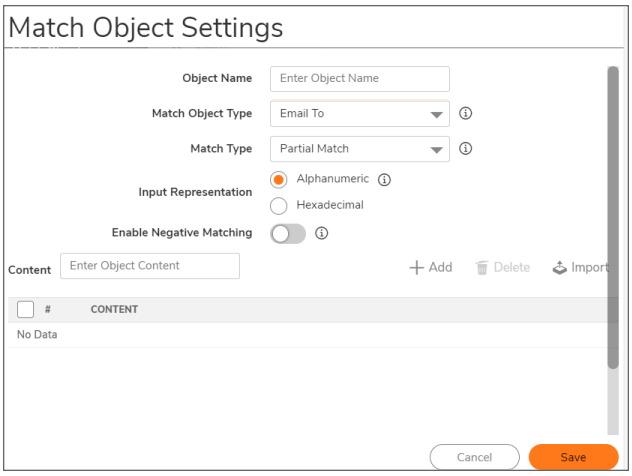
Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a rule, the rule executes actions based on absence of the content specified in the match object.

Multiple list entries in a negative matching object are matched using the logical AND, meaning that the rule action is executed only when all specified negative matching entries are matched.

Although all App Rules are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email *.txt* attachments and block attachments of all other file types or you can allow a few types, and block all others.

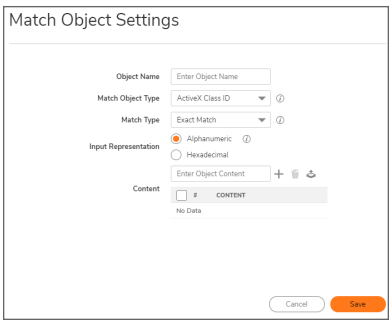
Negative matching option is not available for all type of match object types. You can find the **Enable Negative Matching** option for eligible match object types on the **Match Object Settings** dialog box.



Adding Match Objects

To add a match object:

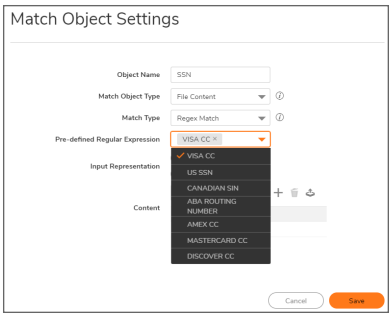
1. Navigate to the **OBJECT | Match Objects > Match Objects**.
2. Click the **Add** icon.



3. Enter a descriptive **Object Name**.
4. Select a **Match Object Type** and **Match Type** from respective drop-down menus. For more information about description of match object type, refer to Supported Match Object Types.

If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and click the type to add it to the List. For more information, refer to Regular Expressions.

You can also type a custom regular expression into the **Content** field and click **Add** icon to add it to the List.



5. Select the **Input representation**.
   - **Alphanumeric** to match a text pattern
   - **Hexadecimal** to match binary content

     You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files.

     For more information about these tools, refer to the Wireshark and Hex Editor.
6. Add the object **Content** in one of the following ways:
   - Enter a pattern to match in the **Content** field and click the **Add** icon.

     The content appears in the List field.

     You can add multiple entries to create a list of **Content** elements to match. All content that you provide in a match object is case-insensitive for matching purposes.
   - Click **Load From File** icon and import a list of elements from a text file.

     Each element in the file must be on a line by itself.

   Multiple entries, either from a text file or entered manually, are displayed in the List. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

   A match object can include a total of not more than 8000 characters. If each element within a match object contains approximately 30 characters, you can enter about 260 elements. The maximum element size is 8000 bytes.
7. Click **Save**.

   New objectis created and listed on the **OBJECT | Match Objects >Match Objects** page with an object type of Application List. You can select this object while creating an App Rules policy or an App Based Route policy.

Editing Match Objects

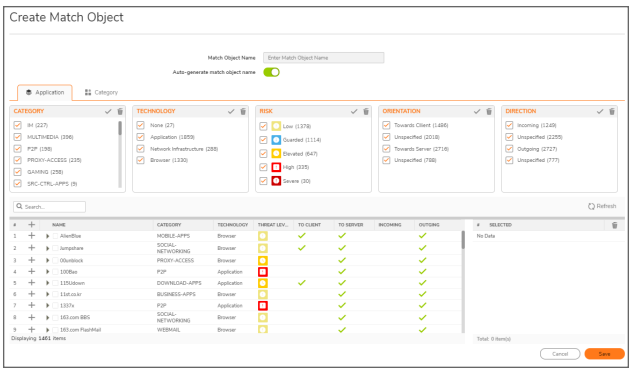
To edit a Match Object:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Hover over the match object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Match Objects.
4. Click **Save**.

Application Objects

From **Match Objects**, you can create two types of application list objects, Application and Category.

- **Application**
  You can create an application filter object on this screen. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The **Application** screen provides one way to create a match object of the **Application List** type. For more information, refer to Adding Application Objects.
- **Category**
  You can create a category filter object on this screen. A list of application categories is displayed, with descriptions that appear when you hover over a category. The **Category** screen allows you to create a match object of the **Application Category List** type. For more information, refer to Adding Category Objects.



Topics:

- Adding Application Objects
- Editing Application Objects
- Adding Category Objects
- Editing Category Objects

Adding Application Objects

This section describes how to create an Application List Object, which can be used by App Rules policies or App Based Route policies.

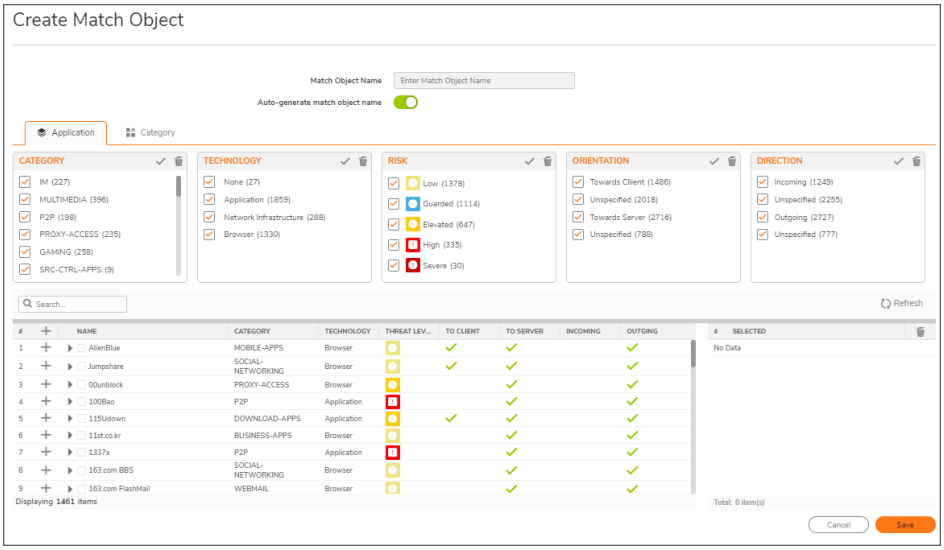
For more information about application list object types including information about the Category screen, refer to Application Objects.

The **Application** page provides a list of applications for selection.

To create an application object:

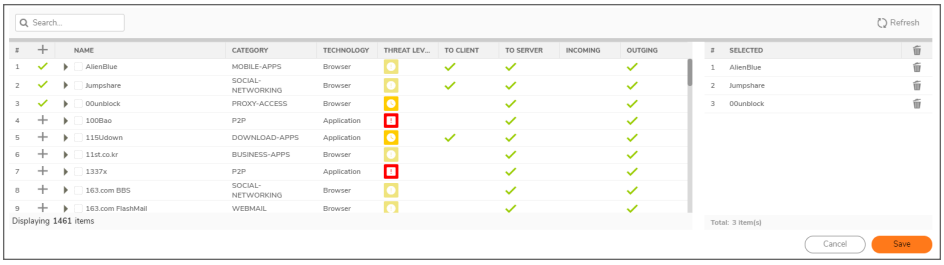
1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Click the **Add Applications** icon.
3. Disable the **Auto-generate match object name** to enter a custom **Match Object Name**.

   NOTE:
   - You can leave the **Auto-generate match object name** enabled if you want to go with auto-generated object name.
   - Application list objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.
4. Click **Applications** tab.



5. Reduce the number of application categories being displayed per below:
   a. Select one or more application categories, technologies, risks, orientation, and direction to filter the applications.
   b. Type a search string in the field.
      For example, type in *bittorrent* into the **Search** field to find multiple applications with *bittorrent* (not case-sensitive) in the name.
6. Click the **Plus** icon next to the application from the filtered list.

   NOTE:
   - Selected applications appear in the **Selected** pane on the right pane.
   - Selected applications turn into green tick mark in the left pane.
7. Click the **Delete** icon of the application to remove the application from the **Selected** pane.
8. Click **Save**.



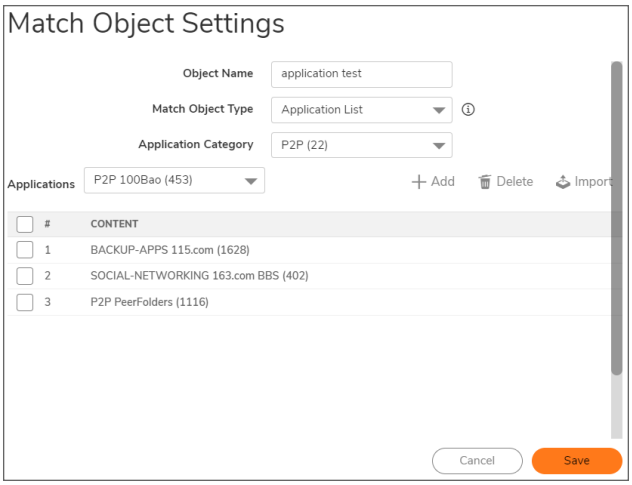
New object is created and listed on the **OBJECT |> Match Objects > Match Objects** page with an object type of Application List. You can select this object while creating an App Rules policy or an App Based Route policy.

Editing Application Objects

To edit an Application Object:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Edit the application list in one of the following ways:
   a. Hover over the application object to be edited and click the **Edit** icon.
      Add the applications to the list:
      1. Set the **Application Category** from the drop-down menu.
      2. Select the **Applications** from the drop-down menu for the selected category in the above step
      3. Click the **Add** icon.

      Remove the applications from the list:
      1. Check **Application** box to be removed from the list.
      2. Click the **Delete** icon.



b. Hover over the application list to be edited and click the **Edit Application List Object** icon.

- Make the necessary changes. For more information, refer to Adding Application Objects.

3. Click **Save**.

Adding Category Objects

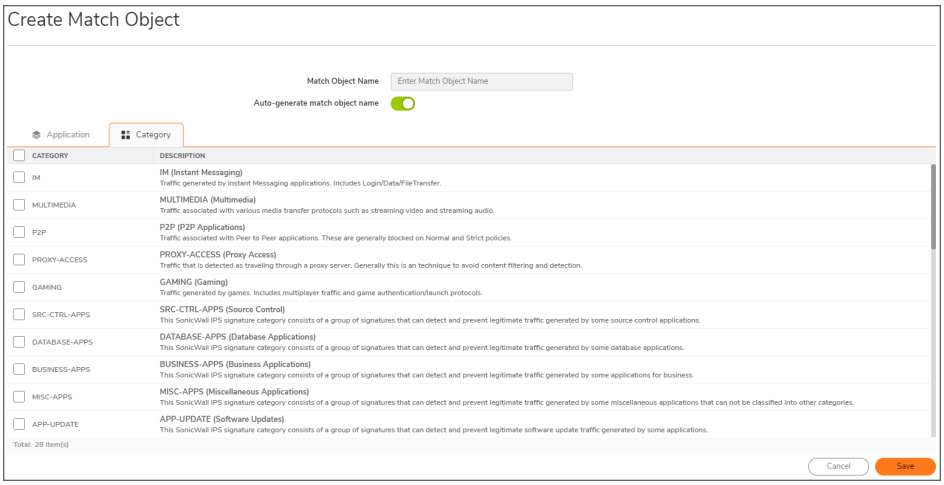
The **Category** page provides a list of application categories for selection. You can select any combination of categories and save your selection as a category filter object with a custom name. The image below shows the dialog with the description of the application categories.

To create a category object:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Click the **Add Applications** icon.
3. Disable the **Auto-generate match object name** to enter a custom **Match Object Name**.

   NOTE:
   - You can leave the **Auto-generate match object name** enabled if you want to go with auto-generated object name.
   - Application list objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

4. Click **Category** tab.



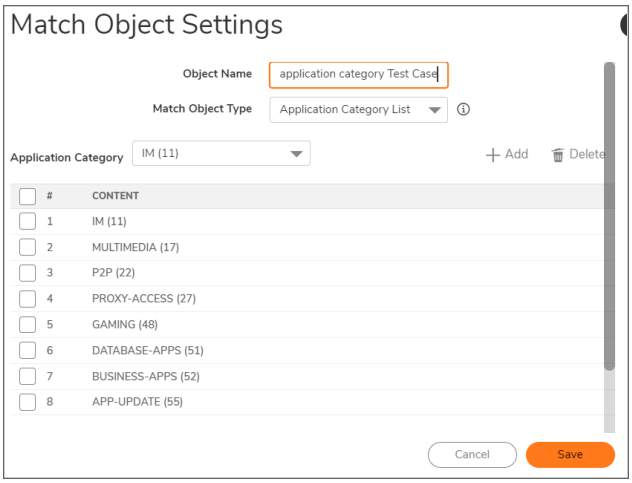
5. Select the check boxes from categories list.
6. Click **Save**.

   New object is created and listed on the **OBJECT |> Match Objects > Match Objects** page with an object type of Application Category List. You can select this object while creating an App Rules policy or an App Based Route policy.

Editing Category Objects

To edit a Category Object:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Edit the application category list in one of the following ways:
   a. Hover over the application category list to be edited and click the **Edit** icon.
      - Select the **Application Category** from the drop-down menu to be added to the list and click the **Add** icon.
      - Check **Application Category** box to be removed from the list and click the **Delete** icon.



b. Hover over the application list object to be edited and click the **Edit Application List Object** icon.

- Check or clear the application category boxes.

3. Click **Save**.

Deleting Match Objects or Application Objects

ⓘ | **NOTE:** You cannot delete an object if it is in use by rule.

To delete a match object or application object:

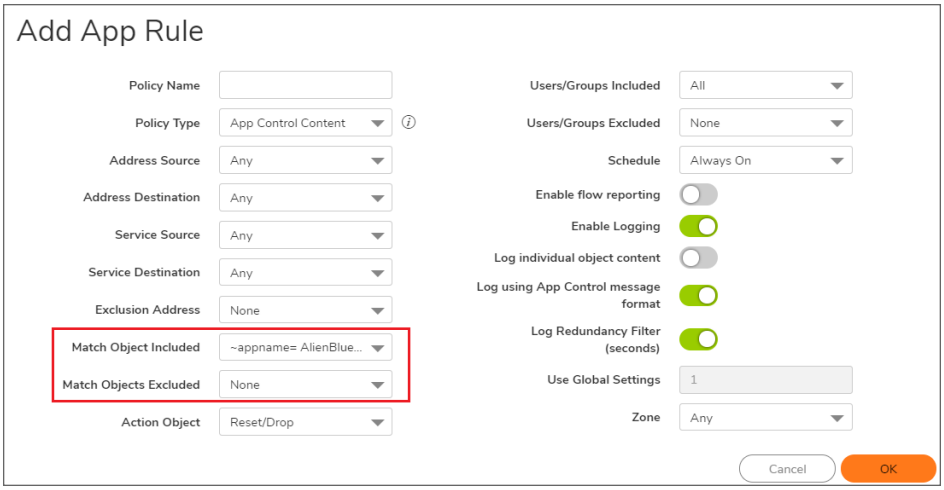
1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Hover over the object to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all match objects or application objects:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Match Objects and Application Objects

Once Match Objects and Application Objects are created on the **OBJECT | Match Objects > Match Objects** page, you can apply these objects while creating an App Rules policy or an App Based Route policy on the **POLICY | Rules and Policies > App Rules** page. For more information, refer to **App Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.



9

Countries

The **Countries** feature is available only in Policy Mode.

From the **Countries** page, you can:

- Filter the table data
- Add, modify, and delete custom groups
- Clone from exiting groups to create a new group
- Refresh and sort the table column data to identify the specific results
- Export the table information into CSV file
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in
- View the list of policies where the Country Group is used.

You can apply the **Country Groups** in defining a security policy on the **POLICY | Rules and Policies > Security Policy** page to allow or block traffic to a group of countries.

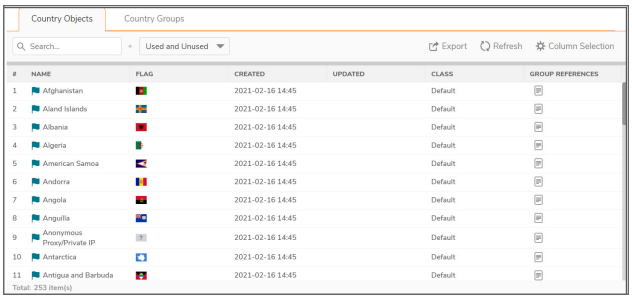
Topics:

Country Objects

Country Objects gives the list of the default objects available to group and apply.

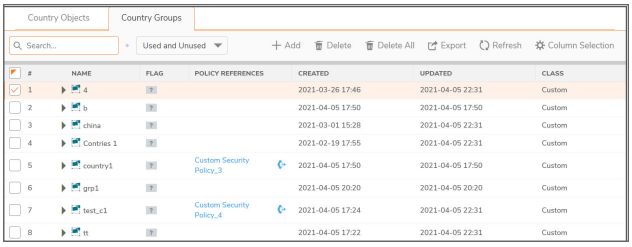
From Country Objects, you can view, export, and refresh the default Country Objects. You can also filter the **Used and/or Unused** in the Country Objects table.

ⓘ | **NOTE:** You cannot add any custom country objects.



Country Groups

SonicOS does not create any default Country Groups. You can create custom groups with any combination of default objects. You can use the country group in policies to apply the same policy for the countries added in that group.



Topics:

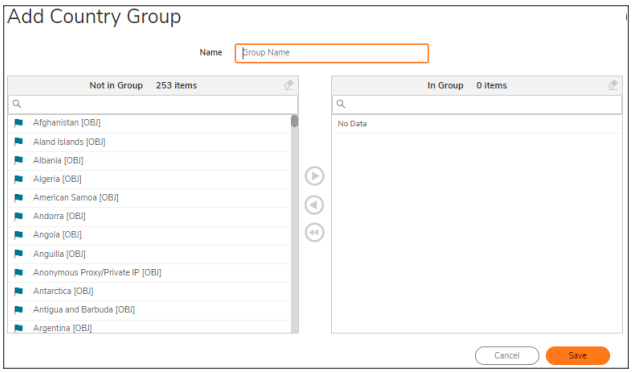
- Adding Country Groups
- Editing Country Groups
- Deleting Custom Country Groups

Adding Country Groups

You can group any combination of countries based on your requirement.

To add a country group:

1. Navigate to **OBJECT | Match Objects > Services > Country Groups**.
2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.
4. Select a country from the **Not in Group** list and click the right arrow to add them to the group.
   Press the **Ctrl** or **Shift** key to select multiple countries.
5. Remove countries from the group in one of the following ways:
   - Select a country from the **In Group** list and click the left arrow to remove the selected country from the group.
   - Click the left double arrow to remove all the countries from the group.
6. Click **Save**.
7. Click the triangle available to the left side of the group **Name** to view the countries included in the group.

Editing Country Groups

To edit a country group:

1. Navigate to **OBJECT | Match Objects > Countries > Country Groups**.
2. Hover over the group to be edited and click the **Edit** icon.
3. Make the necessary changes.
   - Modify name of the group.
   - Add or remove countries.
     For more information, refer to Adding Country Groups.
4. Click **Save**.

Deleting Custom Country Groups

ⓘ | **NOTE:** You cannot delete a group if it is in use by Rule.

To delete a country group:

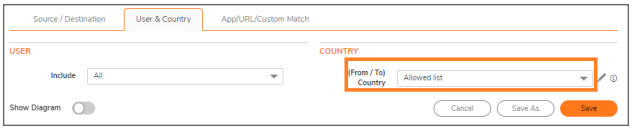
1. Navigate to **OBJECT | Match Objects > Countries > Country Groups**.
2. Set the drop-down menu to **Unused**.
3. Hover over the group to be deleted and click the **Delete** icon.
4. Click **OK** in the confirmation dialog box.

To delete multiple or all country groups:

1. Navigate to **OBJECT | Match Objects > Countries > Country Groups**.
2. Set the drop-down menu to **Unused**.
3. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
4. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Country Groups

Once the Country Groups are created, you can apply the **Country Groups** in defining a security policy on **POLICY | Rules and Policies > Security Policy** page to allow or block traffic to a group of countries. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



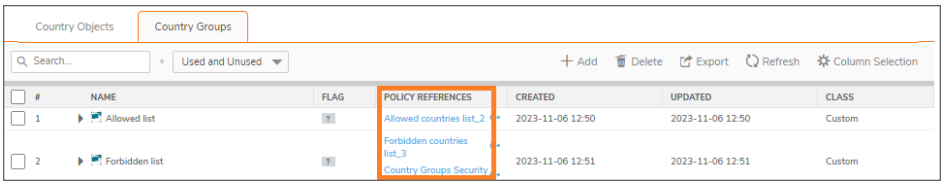
Once the Country Groups are applied to security policies, you can view the list of Security Policies where the Country Group is used.

To view the security policies in use:

1. Navigate to **OBJECT | Match Objects > Countries > Country Groups**.

   Under **POLICY PREFERENCES** column, you can view the security policies where the country group is used .

2. Click the security policy link under the **POLICY PREFERENCES** column to view the policy details.



10

Applications

The Applications feature is available only in Policy Mode. The **Applications** include:

Application Objects	A list of default application objects that are available.
Application Groups	A list of default application groups created based on the **Technology** type. You can also create custom application groups based on your organizational requirements and apply them in policies.

From the **Applications** page, you can:

- Filter the table data
- Add, modify, and delete Application Groups
- Clone from an exiting group to create a new group
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

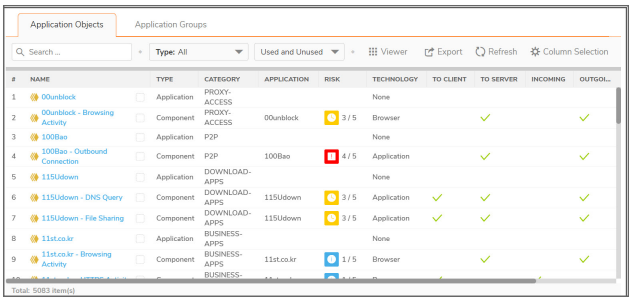
Topics:

Application Objects

Application Objects gives the list of the default objects available to group and apply.

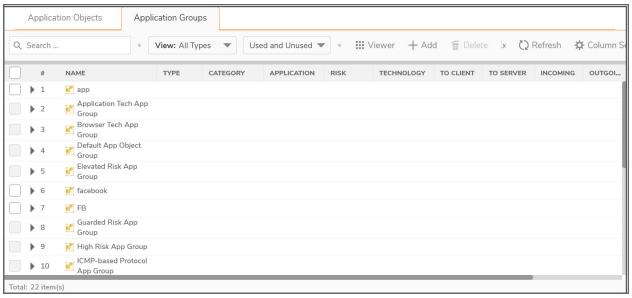
From Application Objects, you can view, export, and refresh the default Application Objects. You can also filter the **Used and/or Unused** in the Application Objects table.

ⓘ | **NOTE:** You cannot add any custom application objects.



Application Groups

The default groups are created by SonicOS. You can use the default groups in policies or create custom groups with any combination of default objects. You can use the group in policies to apply the same policy for the applications added in that group.



Topics:

- Adding Application Groups
- Editing Application Groups
- Deleting Application Groups

Adding Application Groups

You can group any combination of applications based on your requirement.

To add an application group:

1. Navigate to **OBJECT | Match Objects > Applications > Application Groups**.
2. Click the **Add** icon.
3. Enter a descriptive and unique **Name** for the group.
4. Select the items to be included from the **Not in Group** list.
   Press the **Ctrl** or **Shift** key to select multiple items.
5. Click the right arrow to add the selected items to the group.
6. Click **Browse** to select the applications from the **Application Selector** window.
7. Add (+) the required applications from the list and click **Select**.
8. Click **Save**.

Editing Application Groups

ⓘ | **NOTE:** You cannot edit the default application groups.

To edit an application group:

1. Navigate to **OBJECT | Match Objects > Applications > Application Groups**.
2. Set the **View** drop-down menu to **Default**.
3. Hover over the custom group to be edited and click the **Edit** icon.
4. Make the necessary changes.
   - Modify name of the group.
   - Add or remove application objects.
     For more information, refer to Adding Application Groups.
5. Click **Save**.

Deleting Application Groups

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom application group:

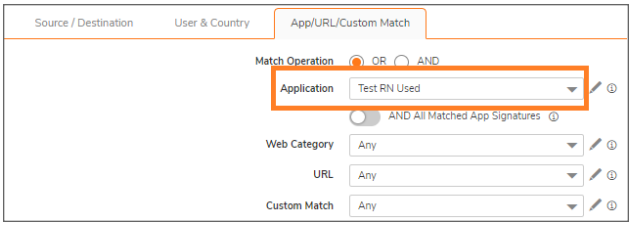
1. Navigate to **OBJECT | Match Objects > Applications**.
2. Set the drop-down menus to **Custom** and **Unused**.
3. Hover over the application group to be deleted and click the **Delete** icon.
4. Click **OK** in the confirmation dialog box.

To delete multiple or all custom application groups:

1. Navigate to **OBJECT | Match Objects > Applications**.
2. Set the drop-down menus to **Custom** and **Unused**.
3. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
4. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Application Groups

Once the **Application Groups** are created, you can apply the **Application Groups** in defining a security policy on **POLICY | Rules and Policies > Security Policy** page based on a group of applications. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



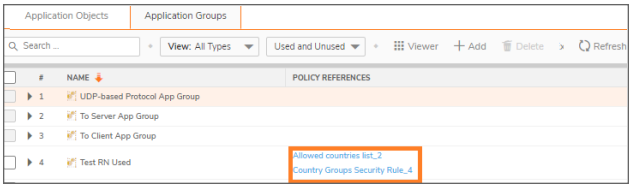
Once the Application Groups are applied in security policies, you can see the list of Security Policies where the Application Group is used.

To view the security policies in use:

1. Navigate to **OBJECT | Match Objects > Applications > Application Groups**.

   Under **POLICY PREFERENCES** column, you can view the security policies where the application group is used.

2. Click the security policy link under the **POLICY PREFERENCES** column to view the policy details.



11

Web Categories

The **Web Categories** feature is available only in Policy Mode. The **Web Categories** include:

Web Category Objects	A list of default web categories that are available.
Web Category Groups	A **Default Web Category Object Group**. You can modify the default group or you can create custom web category groups based on your organizational requirements.

From the **Web Categories** page, you can:

- View the default web category objects and groups
- Filter the table data
- Add, modify, and delete custom web category groups. You can edit the **Default Web Category Object Group** also.
- Clone from an exiting group to create a new group
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in
- View the list of policies where the web category group is used.

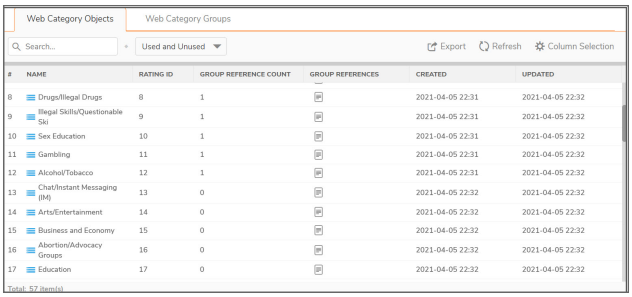
Topics:

Web Category Objects

Web Category Objects gives the list of the default objects available to group and apply.

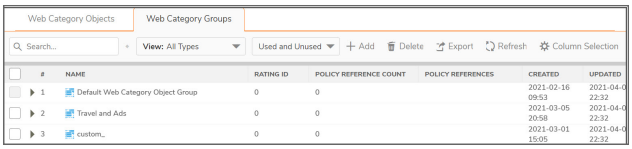
From Web Category Objects, you can view, export, and refresh the default Web Category Objects. You can also filter the **Used and/or Unused** in the Web Category Objects table.

ⓘ | **NOTE:** You cannot add any custom web category objects.



Web Category Groups

The default group **Default Web Category Object Group** is created by SonicOS. You can use the default group in policies or create custom groups with any combination of the default objects. You can use the group in policies to apply the same policy for the web categories added in that group.



Topics:

- Adding Web Category Groups
- Editing Web Category Groups
- Deleting Web Category Groups

Adding Web Category Groups

To add a web category group:

1. Navigate to **OBJECT | Match Objects > Web Categories > Web Category Groups**.
2. Click the **Add** icon.
3. Enter a descriptive and unique **Name** for the group.
4. Select the objects from the **Not in Group** list and click the right arrow to add them to the group.
   Press the **Ctrl** or **Shift** key to select multiple items.
5. Remove objects from the group in one of the following ways:
   - Select an item from the **In Group** list and click the left arrow to remove the selected item from the group.
   - Click the left double arrow to remove all the items from the group.
6. Click **Save**.

Editing Web Category Groups

ⓘ | **NOTE:** You can edit the default group also.

To edit a web category group:

1. Navigate to **OBJECT | Match Objects > Web Categories > Web Category Groups**.
2. Hover over the group to be edited and click the **Edit** icon.
3. Make the necessary changes.
   - Modify name of the group.
   - Add or remove web category objects.
     For more information, refer to Adding Web Category Groups.
4. Click **Save**.

Deleting Web Category Groups

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom web category group:

1. Navigate to **OBJECT | Match Objects > Web Categories**.
2. Set the drop-down menus to **Custom** and **Unused**.
3. Hover over the object to be deleted and click the **Delete** icon.
4. Click **Confirm** in the confirmation dialog box.

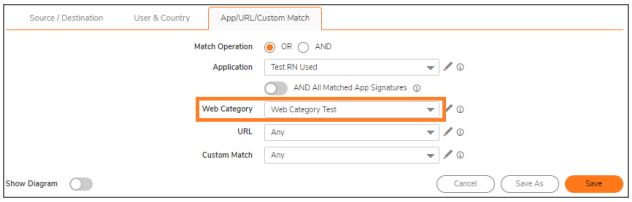
To delete multiple or all custom web category groups:

1. Navigate to **OBJECT | Match Objects > Web Categories**.
2. Set the drop-down menus to **Custom** and **Unused**.
3. Do one of the following:
   - Select check boxes of the web category groups to be deleted and click the **Delete > Selected** icon on top of the table.
   - Click the **Delete > All** icon on top of the table to delete all custom web category groups.
4. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

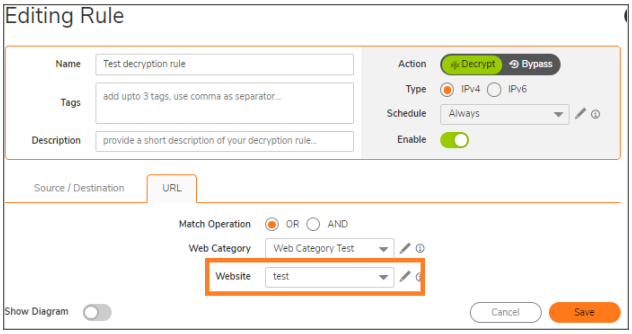
Applying Web Category Groups

Once the Web Category Groups are created, you can apply them in defining:

- A security policy on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



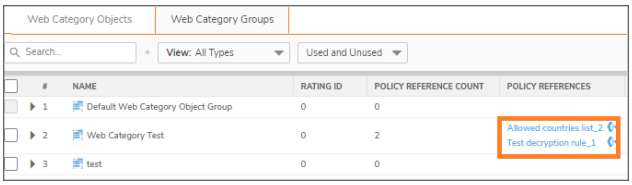
- A decryption policy on **POLICY | Rules and Policies > Decryption Policy** page. For more information, refer to **Decryption Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



Once the Web Category Groups are applied in policies, you can see the list of Policies where the Web Category Group is used.

To view the policies in use:

1. Navigate to **OBJECT | Match Objects > Web Categories > Web Category Groups**.
   Under **POLICY PREFERENCES** column, you can view the policies where the application group is used.
2. Click the policy link under the **POLICY PREFERENCES** column to view the policy details.



12

Websites

SonicOS does not create any default website objects. You can create the objects based on requirements and group them into a single group to use in policies.

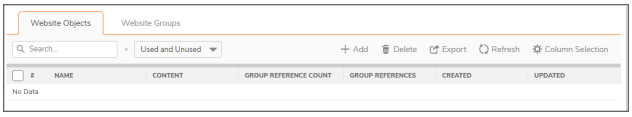
From the **Websites** page, you can:

- Filter the table data
- Add, modify, and delete website objects and groups
- Clone from an exiting group to create a new group
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in
- View the list of policies where the web category group is used.

Topics:

Website Objects

SonicOS does not create any default website objects. You can create website objects based on the requirement.



Topics:

- Adding Website Objects
- Editing Website Objects

Adding Website Objects

To add a Website Object:

1. Navigate to **OBJECT | Match Objects > Websites > Website Objects**.
2. Click the **Add** icon.
3. Enter a descriptive and unique **Name** for the object.
4. Enter the **Domain List** for the Website Object.

To match URL	Input to Domain List field
`www.yahoo.com/*`	**yahoo.in**
`*.yahoo.*/*`	**yahoo**
`*.yahoo.in/*`	**yahoo.in**

ⓘ | **NOTE:** Multiple matches can be added, separated by a comma.

5. Click **Save**.

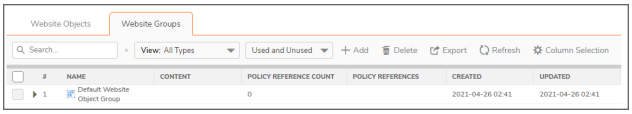
Editing Website Objects

To edit a website object:

1. Navigate to **OBJECT | Match Objects > Websites > Website Objects**.
2. Hover over the object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Website Objects .
4. Click **Save**.

Website Groups

By the default, SonicOS creates the **Default Website Object Group** with no objects. You can either edit the default website group to add the website objects or you can create a custom website groups.



Topics:

- Adding Website Groups
- Editing Website Groups

Adding Website Groups

To add a website group:

1. Navigate to **OBJECT | Match Objects > Websites > Website Groups**.
2. Click the **Add** icon.
3. Enter a descriptive and unique **Name** for the group.
4. Select the objects from the **Not in Group** list and click the right arrow to add them to the group.
   Press the **Ctrl** or **Shift** key to select multiple items.
   Make sure that Website Objects are created to appear in the list.
5. Remove objects from the group in one of the following ways:
   - Select an item from the **In Group** list and click the left arrow to remove the selected item from the group.
   - Click the left double arrow to remove all the items from the group.
6. Click **Save**.

Editing Website Groups

ⓘ | **NOTE:** You can edit the **Default Website Object Group** also.

To edit a website group:

1. Navigate to **OBJECT | Match Objects > Websites > Website Groups**.
2. Hover over the group to be edited and click the **Edit** icon.

3. Make the necessary changes.
    - Modify name of the group.
    - Add or remove website objects.
      For more information about adding or removing countries, refer to Adding Website Groups.
4. Click **Save**.

Deleting Website Objects or Groups

NOTE:
- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom website object or group:

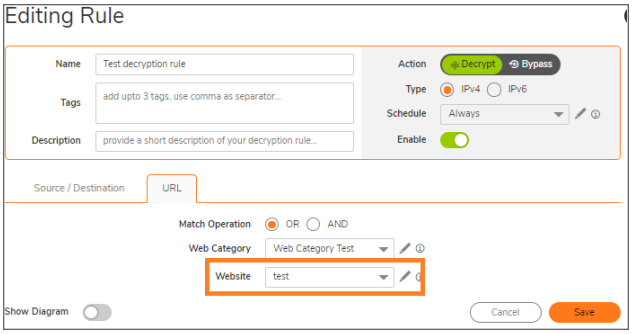
1. Navigate to **OBJECT | Match Objects > Websites**.
2. Click **Website Objects** or **Website Groups** under which you want delete.
3. Set the drop-down menu to **Unused**.
4. Hover over the object or group to be deleted and click the **Delete** icon.
5. Click **Confirm** in the confirmation dialog box.

To delete multiple or all custom website objects or groups:

1. Navigate to **OBJECT | Match Objects > Websites**.
2. Click **Website Objects** or **Website Groups** under which you want delete.
3. Set the drop-down menu to **Unused**.
4. Do one of the following:
    - Select check boxes of the website objects or groups to be deleted and click the **Delete > Selected** icon on top of the table.
    - Click the **Delete > All** icon on top of the table to delete all custom web category groups.
5. Do one of the following:
    a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
    Deletes only unused items and shows the status of each item.
    b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
    Operation gets failed if one of the items is in use by rule.

Applying Website Groups

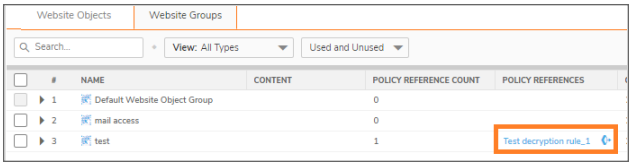
Once the Website Groups are created, you can apply them in defining a decryption policy on **POLICY | Rules and Policies > Decryption Policy** page. For more information, refer to **Decryption Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



Once the Website Groups are applied in policies, you can see the list of policies where the Website Group is used.

To view the policies in use:

1. Navigate to **OBJECT | Match Objects > Website > Website Groups**.
   Under **POLICY PREFERENCES** column, you can view the policies where the application group is used.
2. Click the policy link under the **POLICY PREFERENCES** column to view the policy details.



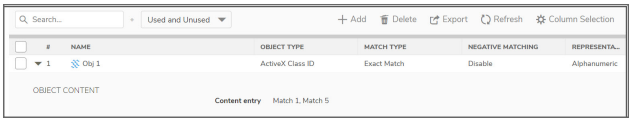
13

Match Patterns

This feature is available only in Policy Mode.

From the **Match Patterns** page, you can:

- Search for the match patterns with a specific string
- Add, modify, and delete match patterns
- Clone from an exiting pattern to create a new pattern
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in



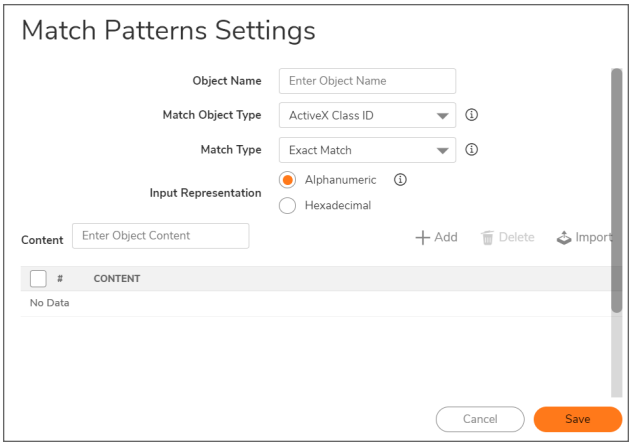
Topics:

- About Match Patterns
- Adding Match Patterns
- Editing Match Patterns
- Deleting Match Patterns
- Applying Match Patterns

About Match Patterns

Match patterns represent the set of conditions which must be matched in order for actions to take place. Match patterns include:

- Match Object Type. For more information, refer to Supported Match Object Types.
- Match Type (exact, partial, regex, prefix, or suffix). For more information, refer to Supported Match Object Types.
- Input representation.
- Actual content to match. The File Content match object type provides a way to match a pattern or keyword within a file.



Topics:

- Input representation
- Supported Match Object Types
- Regular Expressions
- Negative Matching

Input representation

Representation	Used to match	Example
Hexadecimal	Binary content Hexadecimal representation can be used for binary content found in a graphic image.	Executable files

Representation	Used to match	Example
Alphanumeric (text)	Things Alphanumeric (text) can be used to match the same graphic if it contains a certain string in one of its properties fields.	File or email content
Regular expressions (regex)	A pattern rather than a specific string or value Regular expressions (regex) use Alphanumeric input representation.	For more information, refer to Regular Expressions.

Supported Match Object Types

The below table describes the supported match object types and associated match types.

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is **c1fb8842-5281-45ce-a271-8fd5f117ba5**f	Exact	No	None
Custom Object	Allows specification of an IPS-style custom set of conditions	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email	Partial	No	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
Email CC	Any content in the CC MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email From	Any content in the From MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent	N/A	No	None
Email Subject	Any content in the Subject MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
Email To	Any content in the To MIME Header	Exact, Partial, Prefix, Suffix	Yes	None
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed. Provides a way to match a pattern or keyword within a file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.	Partial	No	**Disable attachment** action should never be applied to this object.
File Extension	**For** / **Extension of** Email / An attachment HTTP / An uploaded attachment to the Web mail account FTP / An uploaded or downloaded file	Exact	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
File Name	<table><tr><th>For</th><th>File Name of</th></tr><tr><td>Email</td><td>An attachment</td></tr><tr><td>HTTP</td><td>An uploaded attachment to the Web mail account</td></tr><tr><td>FTP</td><td>An uploaded or downloaded file</td></tr></table>	Exact, Partial, Prefix, Suffix	Yes	None
FTP Command	Allows selection of specific FTP commands	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Cookie	Allows specification of a Cookie sent by a browser	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Host	Content found inside of the HTTP Host header. Represents host name of the destination server in the HTTP request, such as *www.google.com*.	Exact, Partial, Prefix, Suffix	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Referrer	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Set Cookie	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Prefix, Suffix	No	None
HTTP URL	Any HTTP URL that needs to be matched.	Exact, Partial, Prefix, Suffix	No	None
HTTP User Agent	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None

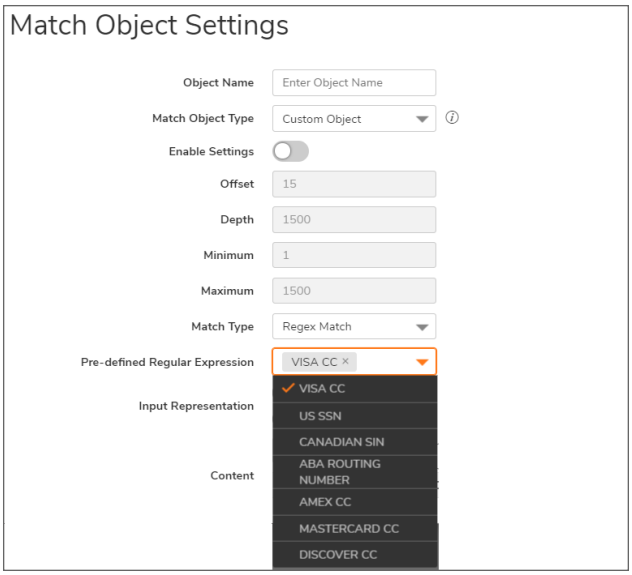
Object Type	Description	Match Types	Negative Matching	Extra Properties
IPS Signature Category List	Available only in Classic Mode. Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures.	N/A	No	None
IPS Signature List	Available only in Classic Mode. Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None
Application Category List	Available only in Classic Mode. Allows specification of application categories, such as Multimedia, P2P, or Social Networking	N/A	No	None
Application List	Available only in Classic Mode. Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Available only in Classic Mode. Allows specification of individual signatures for the application and category that you select	N/A	No	None
Log Email User	Log SMTP E-mail users	N/A	No	None

Regular Expressions

You can configure regular expressions in certain types of match objects for use in App Rules policies. The Match Object Settings options provide a way to configure custom regular expressions or to select from predefined regular expressions. The SonicWall implementation supports reassembly-free regular expression matching on network traffic. This means that no buffering of the input stream is required and patterns are matched across packet boundaries.

SonicOS provides the following predefined regular expressions:

VISA CC	VISA Credit Card Number
US SSN	United States Social Security Number
CANADIAN SIN	Canadian Social Insurance Number
ABA ROUTING NUMBER	American Bankers Association Routing Number
AMEX CC	American Express Credit Card Number
MASTERCARD CC	Mastercard Credit Card Number
DISCOVER CC	Discover Credit Card Number



Policies using regular expressions match the first occurrence of the pattern in network traffic. This enables actions on matches as soon as possible. Because matching is performed on network traffic and not only on human-readable text, the matchable alphabet includes the entire ASCII character set — all 256 characters.

Popular regular expression primitives such as '.', (any character wildcard), '*', '?', '+', repetition count, alternation, and negation are supported. Though the syntax and semantics are similar to popular regular expression implementations such as Perl, vim, and others, there are some minor differences. For example, beginning (^) and end of line ($) operators are not supported. Also, '\z' refers to the set of non-zero digits, [1-9], not to the end of the string as in PERL. For more information about syntax, refer to Regular Expression Syntax.

One notable difference with the Perl regular expression engine is the lack of back-reference and substitution support. These features are actually extraneous to regular expressions and cannot be accomplished in linear time with respect to the data being examined. Hence, to maintain peak performance, they are not supported. Substitution or translation functionality is not supported because network traffic is only inspected, not modified.

Predefined regular expressions for frequently used patterns such as U.S. social security numbers and VISA credit card numbers can be selected while creating the match object. Users can also write their own expressions in the same match object. Such user provided expressions are parsed and any that do not parse correctly will cause a syntax error to display at the bottom of the Match Object Settings window. After successful parsing, the regular expression is passed to a compiler to create the data structures necessary for scanning network traffic in real time.

Regular expressions are matched efficiently by building a data structure called *Deterministic Finite Automaton* (DFA). The DFA's size is dictated by the regular expression provided by the user and is constrained by the memory capacities of the device. A lengthy compilation process for a complex regular expression can consume extensive amounts of memory on the appliance. It may also take up to two minutes to build the DFA, depending on the expressions involved.

To prevent abuse and denial-of-service attacks, along with excessive impact to appliance management responsiveness, the compiler can abort the process and reject regular expressions that cause this data structure to grow too big for the device. An **abuse encountered** error message is displayed at the bottom of the window.

ⓘ **NOTE:** During a lengthy compilation, the appliance management session may become temporarily unresponsive, while network traffic continues to pass through the appliance.

Building the DFA for expressions containing large counters consumes more time and memory. Such expressions are more likely to be rejected than those that use indefinite counters such as the '*' and '+' operators.

Also, at risk of rejection are expressions containing a large number of characters rather than a character range or class. That is, the expression '(a|b|c|d|. . .|z)' to specify the set of all lower-case letters is more likely to be rejected than the equivalent character class '\l'. When a range such as '[a-z]' is used, it is converted internally to '\l'. However, a range such as '[d-y]' or '[0-Z]' cannot be converted to any character class, is long, and may cause the rejection of the expression containing this fragment.

Whenever an expression is rejected, the user may rewrite it in a more efficient manner to avoid rejection using some of the above tips. For more information about syntax, refer to Regular Expression Syntax.

Regular Expression Syntax

This section provides the information about syntax that are used in building regular expressions.

REGULAR EXPRESSION SYNTAX: SINGLE CHARACTERS

Representation	Definition
.	Any character except **\n**. Use **/s** (stream mode, also known as single-line mode) modifier to match **\n** too.
[xyz]	Character class. Can also give escaped characters. Special characters do not need to be escaped as they do not have special meaning within brackets [ ].
\xdd	Hex input. **dd** is the hexadecimal value for the character. Two digits are mandatory. For example, **\r** is **\x0d** and not **\xd**.

Representation	Definition
[a-z][0-9]	Character range.

REGULAR EXPRESSION SYNTAX: COMPOSITES

Representation	Definition
xy	x followed by y
x|y	x or y
(x)	Equivalent to x. Can be used to override precedences.

REGULAR EXPRESSION SYNTAX: REPETITIONS

Representation	Definition
x*	Zero or more x
x?	Zero or one x
x+	One or more x
x{n, m}	Minimum of **n** and a maximum of **m** sequential x's. All numbered repetitions are expanded. So, making m unreasonably large is ill-advised.
x{n}	Exactly n x's
x{n,}	Minimum of n x's
x{,n}	Maximum of n x's

REGULAR EXPRESSION SYNTAX: ESCAPE SEQUENCES

Representation	Definition
\0, \a, \b, \f, \t, \n, \r, \v	**C** programming language escape sequences (**\0** is the NULL character (ASCII character zero)).
\x	Hex-input. **\x** followed by two hexa-decimal digits denotes the hexa-decimal value for the intended character.
***, \?, \+, \(, \), \[, \], \{, \}, \\, \/, \<space>, \#**	Escape any special character. ⓘ **NOTE:** Comments that are not processed are preceded by any number of spaces and a pound sign (#). So, to match a space or a pound sign (#), you must use the escape sequences **** and **\#**.

REGULAR EXPRESSION SYNTAX: PERL-LIKE CHARACTER CLASSES

Representation	Definition
\d, \D	Digits, Non-digits.
\z, \Z	Non-zero digits ([1-9]), All other characters.
\s, \S	White space, Non-white space. Equivalent to [\t\n\f\r]. \v is not included in Perl white spaces.
\w, \W	Word characters, Non-word characters Equivalent to [0-9A-Za-z_].

REGULAR EXPRESSION SYNTAX: OTHER ASCII CHARACTER CLASS PRIMITIVES

If you want...	...then use	
[:cntrl:]	\c, \C	Control character. [\x00 - \x1F\x7F].
[:digit:]	\d, \D	Digits, Non-Digits. Same as Perl character class.
[:graph:]	\g, \G	Any printable character except space.
[:xdigit:]	\h, \H	Any hexadecimal digit. [a-fA-F0-9]. Note this is different from the Perl \h, which means a horizontal space.
[:lower:]	\l, \L	Any lower case character.
[:ascii:]	\p, \P	Positive, Negative ASCII characters. [0x00 – 0x7F], [0x80 – 0xFF].
[:upper:]	\u, \U	Any upper case character.

Some of the other popular character classes can be built from the above primitives. The following classes do not have their own short-hand due of the lack of a nice mnemonic for any of the remaining characters used for them.

REGULAR EXPRESSION SYNTAX: COMPOUND CHARACTER CLASSES

If you want...	... then use	
[:alnum:]	= [\l\u\d]	The set of all characters and digits.
[:alpha:]	= [\l\u]	The set of all characters.
[:blank:]	= [\t<space>]	The class of blank characters: tab and space.
[:print:]	= [\g<space>]	The class of all printable characters: all graphical characters including space.
[:punct:]	= [^\P\c<space>\d\u\l]	The class of all punctuation characters: no negative ASCII characters, no control characters, no space, no digits, no upper or lower characters.
[:space:]	= [\s\v]	All white space characters. Includes Perl white space and the vertical tab character.

REGULAR EXPRESSION SYNTAX: MODIFIERS

Representation	Definition
/i	Case-insensitive
/s	Treat input as single-line. Can also be thought of as stream-mode. That is, dot (**.**) matches **\n** too.

REGULAR EXPRESSION SYNTAX: OPERATORS IN DECREASING ORDER OF PRECEDENCE

Operators	Associativity
[ ], [^]	Left to right
()	Left to right
***, +, ?**	Left to right

Operators	Associativity
. (Concatenation)	Left to right
|	Left to right

Comments in Regular Expressions

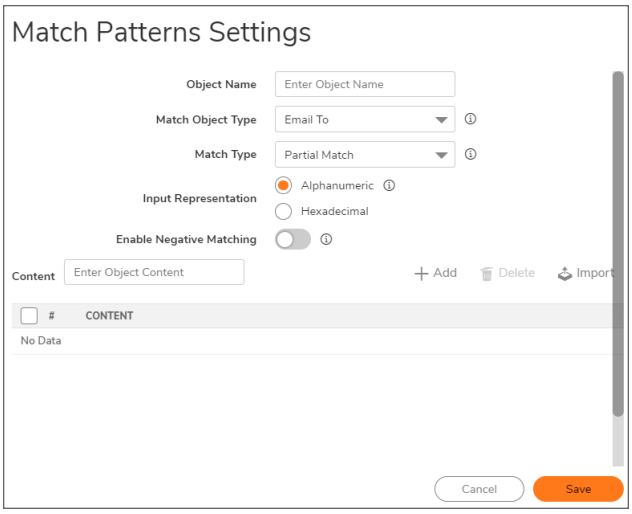
SonicOS supports comments in regular expressions. Comments are preceded by any number of spaces and a pound sign (#). All text after a space and pound sign is discarded until the end of the expression.

Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match pattern when you want to block everything except a particular type of content. When you use the pattern in a policy, the policy executes actions based on absence of the content specified in the match pattern. Multiple list entries in a negative matching pattern are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all security policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email *.txt* attachments and block attachments of all other file types or you can allow a few types, and block all others.

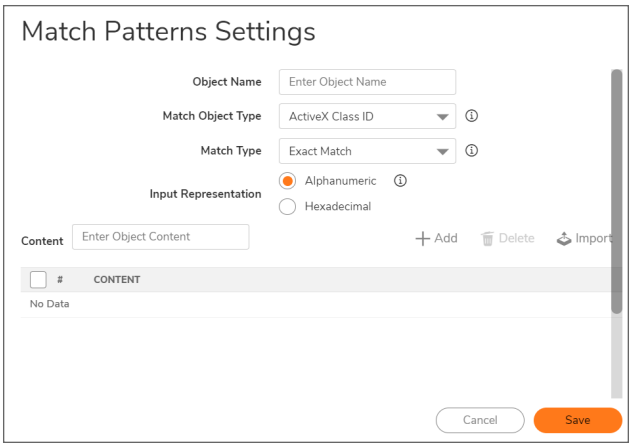
Negative matching option is not available for all type of match object types. You can find the **Enable Negative Matching** option for eligible match object types on the **Match Pattern Settings** dialog box.



Adding Match Patterns

To add a match pattern:

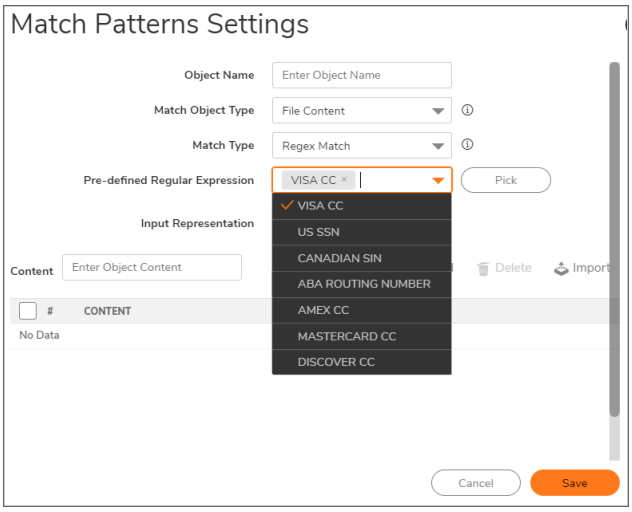
1. Navigate to the **OBJECT | Match Objects > Match Pattern**.
2. Click the **Add** icon.



3. Enter a descriptive **Object Name**.
4. Select a **Match Object Type** and **Match Type** from respective drop-down menus. For more information about description of match object type, refer to About Match Patterns.

   If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and click the type to add it to the List. For more information, refer to Regular Expressions.

   You can also type a custom regular expression into the **Content** field and click **Add** icon to add it to the List.



5. Select the **Input representation**.
    - **Alphanumeric** to match a text pattern
    - **Hexadecimal** to match binary content

      You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files.
6. Add the object **Content** in one of the following ways:
    - Enter a pattern to match in the **Content** field and click the **Add** icon.

      The content appears in the List field.

      You can add multiple entries to create a list of **Content** elements to match. All content that you provide in a match object is case-insensitive for matching purposes.
    - Click **Load From File** icon and import a list of elements from a text file.

      Each element in the file must be on a line by itself.

    Multiple entries, either from a text file or entered manually, are displayed in the List. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

    A match object can include a total of not more than 8000 characters. If each element within a match object contains approximately 30 characters, you can enter about 260 elements. The maximum element size is 8000 bytes.
7. Click **Save**.

    New pattern is created and listed on the **OBJECT | Match Objects > Match Patterns** page. You can select this pattern while creating a custom match object and which in turn can be used in security policies.

Editing Match Patterns

To edit a Match Pattern:

1. Navigate to **OBJECT | Match Objects > Match Patterns**.
2. Hover over the match pattern to be edited and click the **Edit** icon.
3. Make the necessary changes.

    For more information, refer to Adding Match Patterns.
4. Click **Save**.

Deleting Match Patterns

ⓘ | **NOTE:** You cannot delete a pattern if it is in use by a policy.

To delete a match pattern:

1. Navigate to **OBJECT | Match Objects > Match Patterns**.
2. Hover over the item to be deleted and click the **Delete** icon.
3. Click **Confirm** in the confirmation dialog box.

To delete multiple or all match patterns:

1. Navigate to **OBJECT | Match Objects > Match Patterns**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Match Patterns

Once Match Patterns are created on the **OBJECT | Match Objects > Match Patterns** page, you can apply these patterns while creating a Custom Match which in turn can be used in a security policy on the **POLICY | Rules and Policies > Security Policy**. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

14

Custom Match

This feature is available only in Policy Mode.

From the **Custom Match** page, you can:

- Filter the table data for **Used and Unused** objects and groups
- Add, modify, and delete custom match objects and groups
- Clone from an exiting one to create a new one
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in
- View the list of policies where the custom match group is used.

You can configure policies for Client and/or Server Connection Side for incoming and/or outgoing traffic using the objects, Email Addresses, Match Patterns, and group them into a single group to apply them in configuring a security policy. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

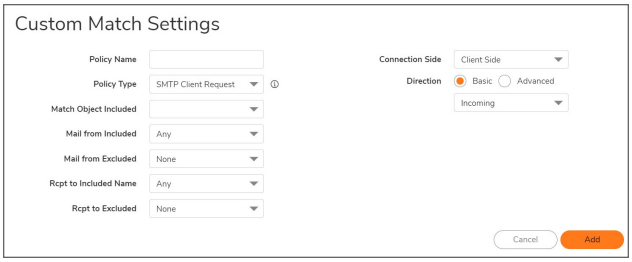
Topics:

Custom Match Objects

From the Custom Match, you can configure match objects with the objects, Email Addresses, Match Patterns based on your requirement which can be grouped to apply in the security policies.

To add a Custom Match Object:

1. Navigate to **OBJECT | Match Objects > Custom Match > Custom Match Objects**.
2. Click the **Add** icon.



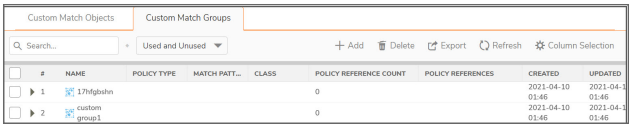
3. Enter a **Policy Name**.
4. Set the policy parameters. You can include the match objects, Email Addresses and Match Patterns based on the policy type selection.
5. Click **Add**.

Custom Match Groups

You can group any combination of Custom Match Objects and custom match groups and apply them in configuring a security policy.

To add a Custom Match group:

1. Navigate to **OBJECT | Match Objects > Custom Match > Custom Match Groups**.
2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.
4. Select the objects or groups from the **Not in Group** list and click the right arrow to add them to the group. Press the **Ctrl** or **Shift** key to select multiple items.

5. Remove objects or groups from the group in one of the following ways:
    - Select an item from the **In Group** list and click the left arrow to remove the selected item from the group.
    - Click the left double arrow to remove all the items from the group.
6. Click **Save**.

Editing Custom Objects or Groups

To edit a custom object or group:

1. Navigate to **OBJECT | Match Objects > Custom Match**.
2. Click the **Custom Match Objects** or **Custom Match Groups** tab which item you want to edit.
3. Hover over the item to be edited and click the **Edit** icon.
4. Make the necessary changes.
5. Click **Save**.

Deleting Custom Objects or Groups

ⓘ | **NOTE:** You cannot delete an object if it is in use by Rule.

To delete a custom match object or group:

1. Navigate to **OBJECT | Match Objects > Custom Match**.
2. Click the **Custom Match Objects** or **Custom Match Groups** tab which item you want to edit.
3. Set the drop-down menu to **Unused**.
4. Hover over the object to be deleted and click the **Delete** icon.
5. Click **Confirm** in the confirmation dialog box.

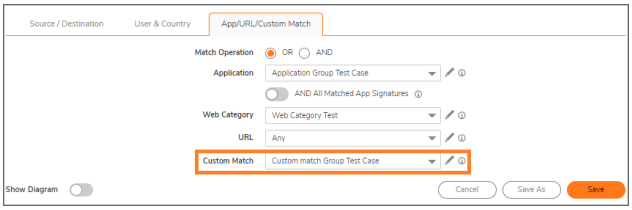
To delete multiple or all custom match objects or groups:

1. Navigate to **OBJECT | Match Objects > Custom Match**.
2. Click the **Custom Match Objects** or **Custom Match Groups** tab which item you want to edit.
3. Set the drop-down menu to **Unused**.
4. Do one of the following:
    - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
    - Select the check box in the table header and click the **Delete** icon on top of the table.
      All custom items get selected.

5. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status. Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Applying Custom Match Groups

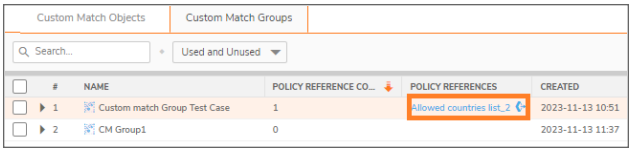
Once the Custom Match Groups are created, you can apply the them in defining a security policy on the **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



Once the groups are applied in security policies, you can see the list of security policies where the group is used.

To view the security policies in use:

1. Navigate to **OBJECT | Match Objects > Custom Match > Custom Match Groups**.
   Under **POLICY PREFERENCES** column, you can view the security policies where the group is used.
2. Click the security policy link under the **POLICY PREFERENCES** column to view the policy details.



2

PROFILE OBJECTS

1

Endpoint Security

With Endpoint Security, you can manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus or Anti Spyware or Capture ATP.

When Endpoint Security is enabled, Capture Client leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection, while providing consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

Endpoint Security can secure your endpoints no matter where they are located and help you keep them clean of malware while enforcing access and content rules.

From **Endpoint Security** page, you can:

- Filter the table data with a specific string
- Add, modify, and delete custom profiles
- Modify the default profile
- Refresh and sort the table columns data to identify the specific results
- Enable or disable the profiles

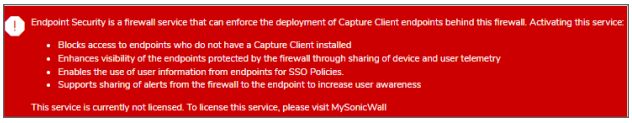
Topics:

Prerequisites

Make sure that:

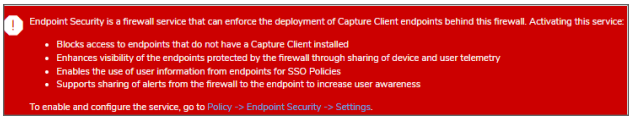
- Capture Client service is licensed under **Endpoint & Remote Access Services** group on **DEVICE | Settings > Licenses** page. For more information, refer to Managing SonicWall Licenses section in SonicOS 7.0 Device Setttings Administration Guide .

  If the license for is not activated, you get error message as shown below.

- **Enable Endpoint Security Enforcement** option is enabled on **POLICY | Endpoint Security** page. For more information, refer to Endpoint Security Administration Guide.

  If the service is not enabled, you get error message as shown below.

Adding Endpoint Security Profiles

A default Endpoint Security Profile, **Endpoint Enforcement Default Profile**, is created by SonicOS with disabled **Capture Client Endpoint Security**. However, you can create a custom Endpoint Security profile based on your requirement.

To add an endpoint security profile:

1. Navigate to **OBJECT | Profile Objects > Endpoint Security**.
2. Click the **Add** icon.
3. Enter a **Name** for the Endpoint Security profile.
4. Set the toggle keys.

Toggle key	Description
Bypass Guest Endpoint Security Service	To bypasses guest check for Endpoint Security when guest service is enabled on matched zone.
Capture Client Endpoint Security	To enable Capture Client endpoint security.

5. Click **Save**.
6. Click **Cancel** to go back to **Endpoint Security** table.

Editing Endpoint Security Profiles

ⓘ | **NOTE:** You can edit the default endpoint security profile also but you cannot change name of it.

To edit an endpoint security profile:

1. Navigate to **OBJECT | Profile Objects > Endpoint Security**.
2. Hover over the profile to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Endpoint Security Profiles.
4. Click **Save**.

Deleting Endpoint Security Profiles

ⓘ | **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

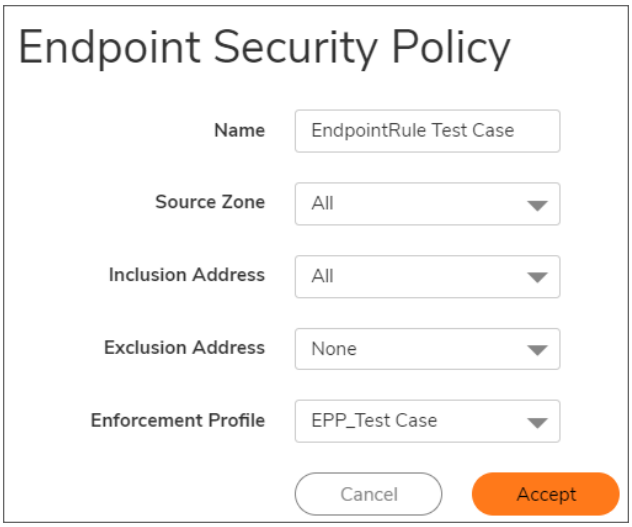
To delete Endpoint Security profiles:

1. Navigate to **OBJECT | Profile Objects > Endpoint Security**.
2. Do one of the following:
   - Hover over the object to be deleted and click the **Delete** icon.
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Click **Confirm**.

Applying Endpoint Security Profiles

Once the endpoint security profiles is configured, you can apply them in configuring Endpoint Rules or Policies on **POLICY | Rule and Policies > Endpoint Rules** page. For more information, refer to:

- Classic Mode: **Endpoint Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
- Policy Mode: **Endpoint Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.



2

Bandwidth

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network through the use of an established use profile.

SonicOS offers an integrated traffic shaping mechanism through its outbound (Egress) and inbound (Ingress) BWM interfaces.

Egress BWM	It can be applied to traffic sourced from Trusted and Public zones traveling to Untrusted and Encrypted zones.
Ingress BWM	It can be applied to traffic sourced from Untrusted and Encrypted zones traveling to Trusted and Public zones.

The SonicWall security appliance uses BWM to control ingress and egress traffic. BWM allows network administrators to guarantee minimum bandwidth and prioritize traffic based on policies created in the **OBJECT | Profile Objects > Bandwidth** page of the management interface. By controlling the amount of bandwidth to an application or user, you can prevent a small number of applications or users to consume all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance.

ⓘ **NOTE:** Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single SonicWall appliance, effectively eliminating the dependency on external systems thereby obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule (Classic Mode) or Security Action Profile (Policy Mode). This allows those external systems to benefit from the classification performed on the firewall even after it has already shaped the traffic. For more information about BWM QoS details, refer to Applying QoS Marking.

BWM Traffic Priority Queues list the SonicOS traffic priority queues.

BWM TRAFFIC PRIORITY QUEUES

0 – Realtime	3 – Medium High	6 – Low
1 – Highest	4 – Medium	7 – Lowest
2 – High	5 – Medium Low	

BANDWIDTH MANAGEMENT TYPES

BWM Type	Description
Advanced	Enables Advanced Bandwidth Management. Maximum egress and ingress bandwidth limitations can be configured on any interface, per interface, by configuring bandwidth objects, access rule (Classic Mode) or security action profile (Policy Mode), and application policies and attaching them to the interface.
Global	All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed according to the priority queue. Default Global BWM queues: 2 High 4 Medium 6 Low 4 Medium is the default priority for all traffic that is not managed by an access rule or an application control policy or a security policy that is BWM enabled. For traffic more than 1 Gbps, maximum bandwidth is limited to 1 Gbps because of queuing, which may limit the number of packets processed.
None	(Default) Disables BWM.

If the bandwidth management type is **None**, and there are three traffic types that are using an interface, if the link capacity of the interface is 100 Mbps, the cumulative capacity for all three types of traffic is 100 Mbps.

When **Global** bandwidth management is enabled on an interface, all traffic to and from that interface is bandwidth managed. If the available ingress and egress traffic is configured at 10 Mbps, then by the default, all three traffic types are sent to the medium priority queue. The medium priority queue, by the default, has a guaranteed bandwidth of 50 percent and a maximum bandwidth of 100 percent. If no **Global** bandwidth management policies are configured, the cumulative link capacity for each traffic type is 10 Mbps.

ⓘ **NOTE:** BWM rules consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS is limited by platform (values are subject to change).

Global uses the unused guaranteed bandwidth from other queues for maximum bandwidth. If there is only default or single-queue traffic and all the queues have a total of 100% allocated as guaranteed, **Global** uses the unused global bandwidth from other queues to give you up to maximum bandwidth for the default or single-queue.

From **Bandwidth** page, you can:

- Filter the table data with a specific string, default and custom profiles
- Add, modify, and delete custom profiles
- Modify the default profile
- Refresh and sort the table columns data to identify the specific results

Topics:

- Configuring Bandwidth Profile Objects
- Editing Bandwidth Profile Objects
- Deleting Bandwidth Profile Objects
- Applying Bandwidth Profile Objects

Configuring Bandwidth Profile Objects

Bandwidth profile objects are based on policies that specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts:

- A classifier
- A bandwidth rule

A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth profile object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

Configuring the bandwidth profile object includes:

- Defining Bandwidth Profile Object Settings
- Enabling BWM on an Interface

Defining Bandwidth Profile Object Settings

Defining Bandwidth Profile Object includes, setting up:

- General Settings of Bandwidth Profile Object
- Elemental Settings of Bandwidth Profile Object

General Settings of Bandwidth Profile Object

General section of the bandwidth configuration defines guaranteed and maximum bandwidth, traffic priority, and violation action.

To configure a BWM configuration:

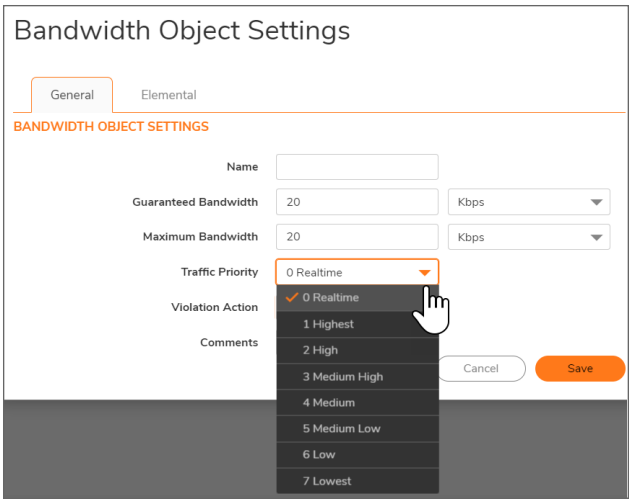
1. Navigate to the **OBJECT | Profile Objects > Bandwidth**.

   NOTE:
   - The default settings for this page consists of three priorities with pre-configured guaranteed and maximum bandwidth. The medium priority has the highest guaranteed value as this priority queue is used by the default for all traffic not governed by a BWM-enabled policy.

- The default values are set by SonicWall to provide BWM ease-of-use. It is recommended to review your specific bandwidth needs and update the values on this page accordingly.

2. Click the **Add** icon.

   By the default, **General** tab of the Bandwidth Object Settings displays.



3. Enter a **Name** for the BWM configuration.
4. Enter the Bandwidth values.

Guaranteed Bandwidth	To provide guaranteed bandwidth for a particular traffic class.
Maximum Bandwidth	To provide maximum bandwidth that a traffic class can utilize.

ⓘ **NOTE:** The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

5. Select the **Traffic Priority**.
   - The highest priority is 0 Real time which is the default. The lowest priority is 7 Lowest.
   - When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.
   - For more information, refer to Bandwidth.
6. Set the **Violation Action** for the firewall that occurs when traffic exceeds the maximum bandwidth.

Delay (Default)	Excess traffic packets are queued and sent when possible.
Drop	Excess traffic packets are dropped immediately.

7. Enter **Comments** for the bandwidth object if you wish to add any.
8. Click **Save**.

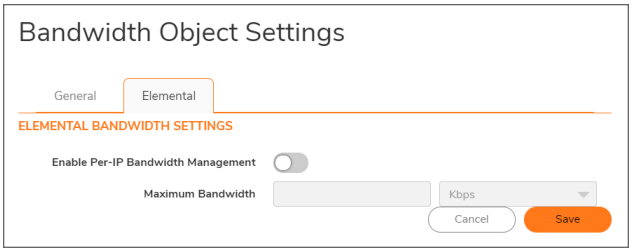
Elemental Settings of Bandwidth Profile Object

Elemental bandwidth object settings provide a method of allowing a single BWM rule to apply to the individual elements of that rule. Per-IP Bandwidth Management is an **Elemental** feature that is a sub-option of **Bandwidth Object Settings**. When Per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule or traffic class.

The Elemental Bandwidth Object Settings option enables a bandwidth object to be applied to individual elements under a parent traffic class.

To configure an Elemental Bandwidth Object Settings:

1. Navigate to the **OBJECT | Profile Objects > Bandwidth**.
2. Do one of the following:
   a. Click the **Add** icon.
      Enter a **Name** for the BWM configuration.
   b. Hover over an existing Bandwidth Object from the table and click the **Edit** icon.
3. Click the **Elemental** tab.



4. **Enable Per-IP Bandwidth Management**.
5. Enter the **Maximum Bandwidth** in Kbps (default) or Mbps.
6. Click **Save**.

Enabling BWM on an Interface

Enable BWM on an interface according to **Interfaces > Interface Settings IPv4 > Enabling Bandwidth Management on an Interface** section in SonicOS 7.0 System Administration Guide .

Editing Bandwidth Profile Objects

ⓘ **NOTE:** You can edit the default bandwidth profile objects to modify the attributes except **Name** and **Comments**.

To edit a Bandwidth Profile Object:

1. Navigate to the **OBJECT | Profile Objects > Bandwidth**.
2. Hover over the Bandwidth Profile Object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   You cannot modify **Name** and **Comments** for the default Bandwidth Profile Object.
4. Click **Save**.

Deleting Bandwidth Profile Objects

ⓘ **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom bandwidth profile object:

1. Navigate to the **OBJECT | Profile Objects > Bandwidth**.
2. Hover over the custom bandwidth profile object to be deleted and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom bandwidth profile objects:

1. Navigate to the **OBJECT | Profile Objects > Bandwidth**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.

b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Applying Bandwidth Profile Objects

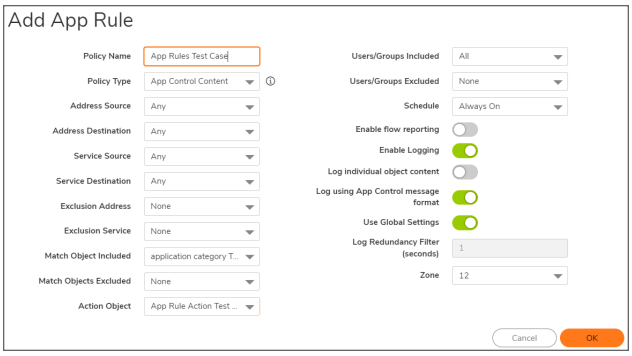
Once the bandwidth profile object is configured, you can apply the bandwidth profile object to configure:

In Classic Mode:

- CFS BWM Action Objects on **OBJECT | Action Profiles > Content Filter Actions** page. For more information, refer to BWM.
- **App Rule Actions** on **OBJECT | Action Objects > App Rule Actions** page. For more information, refer to Adding Action Objects. These App Rule Actions can be used to configure:
  - **Access Rules** in **Traffic Shaping** on **POLICY | Rules and Policies > Access Rules** page.

    For more information, refer to **Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
  - **App Rules** on **POLICY | Rules and Policies > App Rules** page.

    Classic Mode: Create an access rule on the **POLICY | Rules and Policies > App Rules** page. For more information, refer to **App Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.



In Policy Mode:

- **Security Action Profiles** on **OBJECT | Action Profiles > Security Action Profile** page. For more information, refer to Configuring a Bandwidth/QoS Security Action Profile.

  These Security Action Profiles can be used to configure a security policy on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

3

QoS Marking

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic and guarantee the desired levels of network service.

This section includes:

- Classification of traffic
- Marking of traffic once the traffic is classified
- Conditioning or managing methods of traffic
- Tags of QoS marking, 802.1p and DSCP QoS
- Mapping of QoS Tags
- Configuring QoS Marking
- Applying QoS Marking

Classification

Classification is necessary as a first step so that traffic in need of management can be identified.

For classification of traffic, SonicOS uses:

- Access Rules as the interface in Classic Mode. For more information, refer to **Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
- Security Policy as the interface in Policy Mode. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from host A to server B on Wednesdays at 2:12am**.

SonicWall network security appliances have the ability to recognize, map, modify, and generate the industry-standard external CoS (Class of Service) designators, DSCP (Differentiated Services Code Point) and 802.1p. For more information, refer to 802.1p and DSCP QoS.

When identified or classified, traffic can be managed. Management can be performed internally by SonicOS Bandwidth Management (BWM), which is effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced such as foreign network infrastructures with unknown configurations or other hosts contending for bandwidth (for example, the Internet), the ability to offer guarantee and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM works exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. After SonicOS classifies the traffic, it can *tag* the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags, thus they too can participate in providing QoS.

NOTE:

- Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations are not able to recognize 802.1p tags, and could drop tagged traffic.
- Although DSCP does not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.
- If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider, some offer fee-based support for QoS using these CoS methods.

Marking

After the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS aware switches or routers as might be available on a premium service provider's infrastructure or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it rarely mistreats or discards the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p only works with 802.1p capable equipment, and is not universally

interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (such as WAN links) was introduced in the form of 802.1p to DSCP mapping.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. For more information, refer to 802.1p and DSCP QoS.

Conditioning

You can condition or manage the traffic with the help of any of the available methods, policing, queuing, and shaping. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM). SonicOS's BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to DSCP marking: Example scenario in 802.1p Marking for a description of contention issues.

Topics:

- Site to Site VPN over QoS Capable Networks
- Site to Site VPN over Public Networks

Site to Site VPN over QoS Capable Networks

If the network path between the two endpoints is QoS aware, SonicOS can DSCP tag:

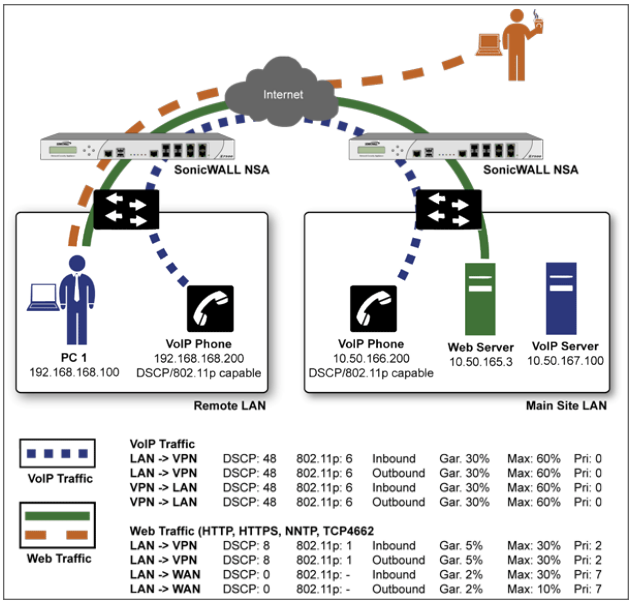
- The inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel.
- The outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network.

SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. When the packets are received on the other side, the receiving SonicWall appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non-QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

SITE TO SITE VPN OVER PUBLIC NETWORKS



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP.

SonicOS has the ability to:

- DSCP mark traffic after classification
- Map 802.1p tags to DSCP tags for external network traversal and CoS preservation.

For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

There are two methods of QoS.

802.1p Class of Service is typically used for internal Layer 2 and some Layer 3 mapping. This marking typically will not survive being sent to the Public Internet and isn't universally supported.

DSCP Marking is used for Layer 2 and Layer 3 mapping. Not all networking devices or ISPs support DSCP Class of Service.

Topics:

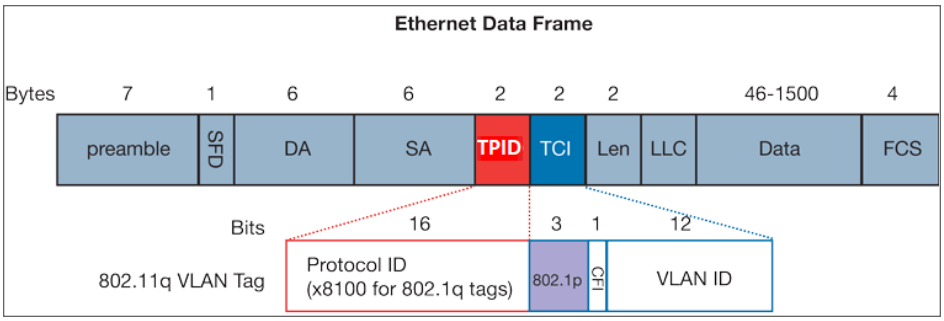
- 802.1p Marking
- DSCP Marking

802.1p Marking

SonicOS supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments.

The layer 2 method is the IEEE 802.1p standard. The standard uses a three-bit field within an Ethernet frame header to assign priority levels to packets moving within a network segment. With the technique, this priority value is used to differentiate traffic as illustrated in the following figure.

ETHERNET DATA FRAME



TPID	Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ether type of 0x8100 for tagged traffic.
802.1p	The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.

CFI	Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
VLAN ID	VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^12) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

Enable 802.1p marking on any Ethernet interface of the SonicWall appliance to support 802.1p tags. You can control the behavior of the 802.1p field within these tags with Access Rules (Classic Mode) or Security Action Profiles (Policy Mode). The default 802.1p action of None will reset existing 802.1p tags to zero (0), unless otherwise configured. For more information, refer to Applying QoS Marking.

Enabling 802.1p marking allows the target interface:

- To recognize incoming 802.1p tags generated by 802.1p capable network devices.
- To generate 802.1p tags, as controlled by Access Rules (Classic Mode) or Security Action Profiles (Policy Mode).

Frames that have 802.1p tags inserted by SonicOS bears VLAN ID 0.

Enabling 802.1p marking on an interface does not create the 802.1p tags. These tags are inserted according to Access Rules (Classic Mode) or Security Policies (Policy Mode) only. By the 802.1p marking default settings, SonicOS disrupt communications with 802.1p-incapable devices.

Specific support is required from the networking devices to use 802.1p method for prioritization.

- Many voice and video over IP devices provide support for 802.1p, make sure that the feature is enabled.
- Check your equipment's documentation for information on 802.1p support if you are unsure.
- Many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by the default. Make sure that the feature is enabled.
- On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** view of the Properties page of your network card. If your card supports 802.1p, it is listed as **802.1p QoS, 802.1p Support, QoS Packet Tagging** or something similar.

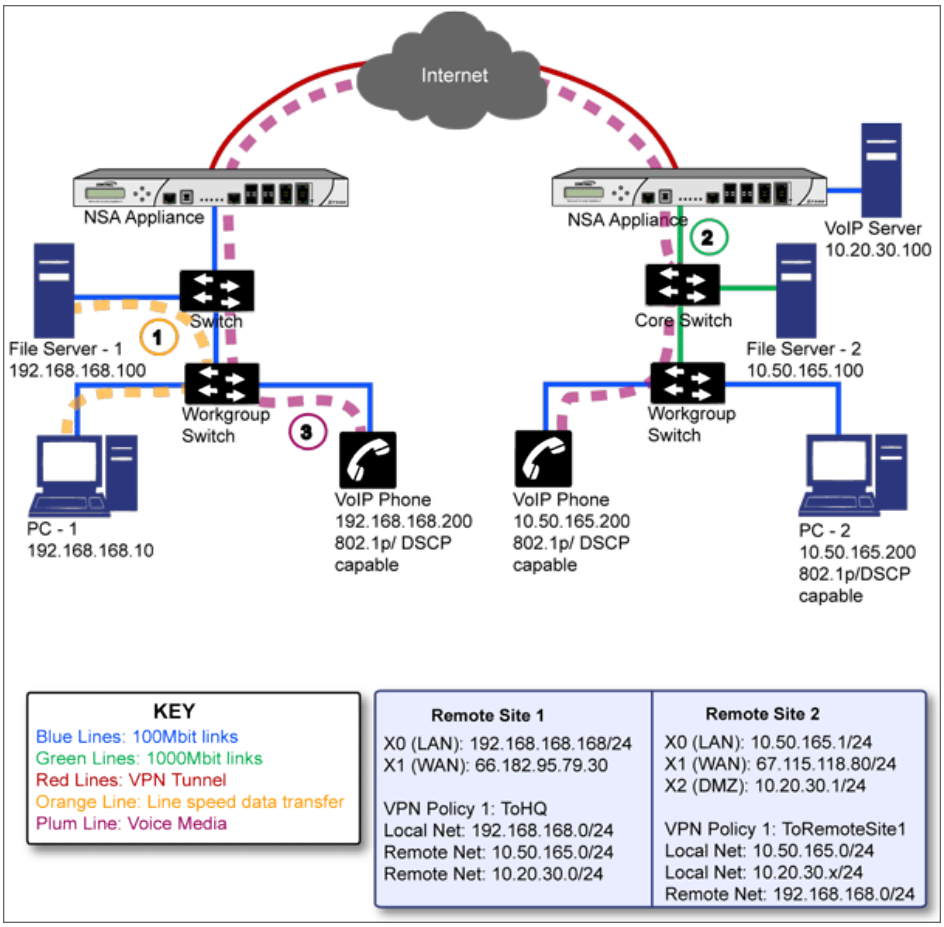
If your network interface supports the 802.1p feature, make sure that the feature is present and enabled on the network interface and then only the network interface can generate packets with 802.1p tags, as governed by QoS capable applications. By the default, general network communications does not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

If your network interface does not support 802.1p, it is not able to process 802.1p tagged traffic, and ignores it. Make sure when defining Access Rules (Classic Mode) or Security Action Profiles and Security Policies(Policy Mode) to enable 802.1p marking that the target devices are 802.1p capable.

ⓘ **NOTE:** When performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices do not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device almost invariably shows the header, but the host is unable to process the packet.

It is important to introduce *DSCP Marking* because of the potential interdependency between the two marking methods, 802.1p and DSCP as well as to explain why the interdependency exists. For more information, refer to QoS Marking Actions.

DSCP MARKING: EXAMPLE SCENARIO



In DSCP marking: Example scenario, we have Remote Site 1 connected to **Main Site** by an IPsec VPN. The company uses an internal 802.1p or DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p or DSCP capable VoIP Phone `10.50.165.200` initiates a call to the person at VoIP phone `192.168.168.200`. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
    a. If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this

behavior varies from switch to switch, and is often configurable.

b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

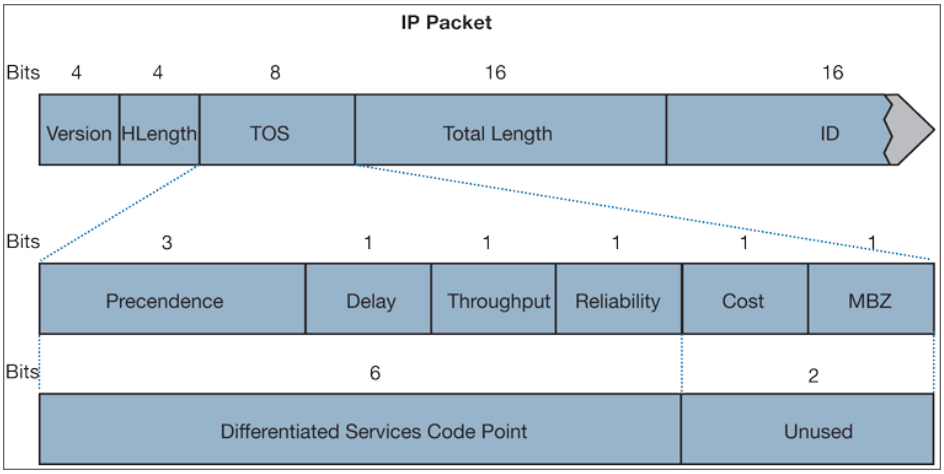
In our above scenario, the firewall at the Main Site assigns a DSCP tag (for example, value 48) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWall, mapping the DSCP tag back to an 802.1p tag.

3. The receiving SonicWall at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the firewall, it bears 802.1p tag 6. The Switch recognizes it as voice traffic, and prioritizes it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

Differentiated Services Code Point (DSCP) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Because DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP simply ignores the tags, or at worst, they reset the tag value to 0.

DSCP MARKING: IP PACKET



DSCP marking:

- IP packet depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.
- Commonly used code points shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP MARKING: COMMONLY USED CODE POINTS

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/Elliptic Curve Group – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/Elliptic Curve Group – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules (Classic Mode) or Security Policies (Policy Mode), from the QoS view, and can be used in conjunction with 802.1p marking, as well as with SonicOS's internal bandwidth management.

Topics:

- DSCP Marking and Mixed VPN Traffic
- Configure for 802.1p CoS 4 – Controlled Load

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS provides a replay window of 64 packets, such as whether an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet is dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (for example, VoIP), and some that is DSCP tagged low-priority, or untagged or best-effort (for example, FTP), your service provider prioritizes the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWall's anti-replay defenses.

If symptoms of such a scenario emerge (for example, excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (for example, the VoIP network) on their own subnet.

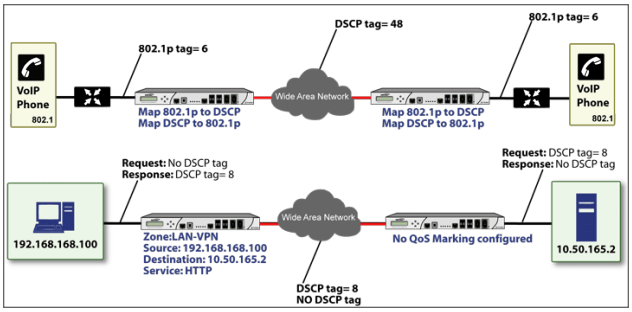
Configure for 802.1p CoS 4 – Controlled Load

If you want to change the inbound mapping of DSCP tag 15 from its default 802.1p mapping of 1 to an 802.1p mapping of 2, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping returns the error: **DSCP range already exists or overlaps with another range**. First, you have to remove 15 from its current end-range mapping to 802.1p CoS 1 (changing the end-range

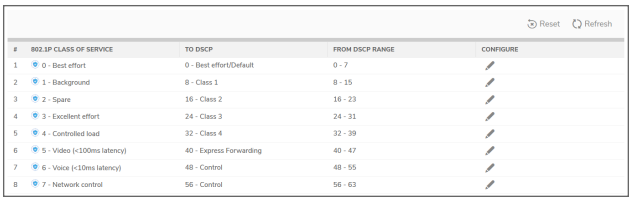
mapping of 802.1p CoS 1 to DSCP 14), then you can assign DSCP 15 to the start-range mapping on 802.1p CoS2.

Mapping of QoS Tags

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (for example, WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side, as shown below.



ⓘ **NOTE:** Mapping does not occur until you assign Map as an action of the QoS view of Access Rules (Classic Mode) or Security Action Profiles (Policy Mode). The mapping table only defines the correspondence that is employed by an Access Rules (Classic Mode) or Security Action Profiles (Policy Mode)'s Map action.



Reset Refresh

#	802.1P CLASS OF SERVICE	TO DSCP	FROM DSCP RANGE	CONFIGURE
1	0 - Best effort	0 - Best effort/Default	0 - 7	
2	1 - Background	8 - Class 1	8 - 15	
3	2 - Spare	16 - Class 2	16 - 23	
4	3 - Excellent effort	24 - Class 3	24 - 31	
5	4 - Controlled load	32 - Class 4	32 - 39	
6	5 - Video (<100ms latency)	40 - Express Forwarding	40 - 47	
7	6 - Voice (<10ms latency)	48 - Control	48 - 55	
8	7 - Network control	56 - Control	56 - 63	

For example, according to the default table, an 802.1p tag with a value of **2** is outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** is inbound mapped to an 802.1 value of **5**.

Each of these mappings can be reconfigured. For more information, refer to Configuring QoS Marking.

Configuring QoS Marking

From the Profile Objects, you can only view and edit the QoS Marking mappings for 802.1p and DSCP tags.

To modify Quality of Service (QoS) Marking packets:

1. Navigate to **OBJECT | Profile Objects > QoS Marking**.
2. Hover over the QoS Marking profile to be edited and click the **Edit** icon.

If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of 43, hover over **4 – Controlled load** and click **Edit** icon.

3. Select new **To DSCP** value from the drop-down menu and other necessary changes.
4. Click **Update**.

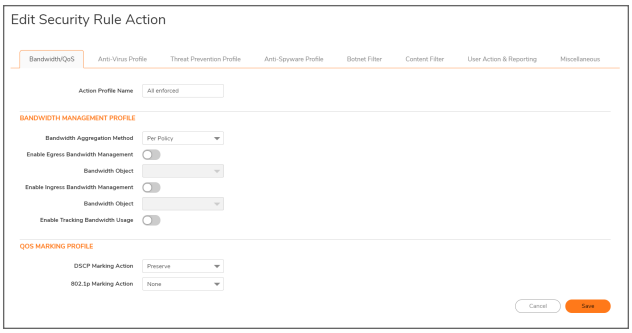
Applying QoS Marking

You can manage the QoS marking profile as described below:

- In Policy Mode: You can manage the QoS marking in **Security Action Profiles** under **Bandwidth/QoS** tab on **OBJECT | Action Profiles > Security Action Profile** page.

  For more information:

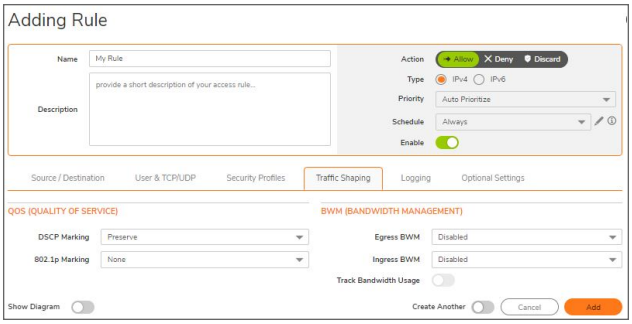
  - About **Bandwidth/QoS**, refer to Configuring a Bandwidth/QoS Security Action Profile.
  - About marking actions, refer to QoS Marking Actions.



- In Classic Mode: You can manage the QoS marking in **Access Rules** under **Traffic Shaping** tab on **POLICY | Rules and Policies > Access Rules** page.

  For information about:

  - About **Traffic Shaping**, refer to **Access Rules > Setting Firewall Access Rules > Configuring Access Rules** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.
  - Marking actions, refer to QoS Marking Actions.



Topics:

- QoS Marking Actions
- Bi-directional DSCP Tag Action

QoS Marking Actions

Both 802.1p and DSCP markings are managed by SonicOS Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) provide four actions: **None**, **Preserve**, **Explicit**, and **Map**.

The default action for DSCP is **None** and the default action for 802.1p is **Preserve**.

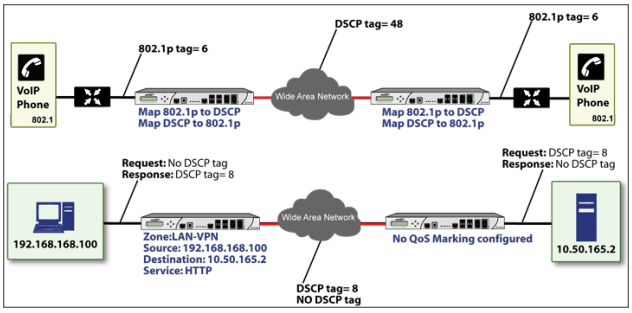
QoS marking behavior describes the behavior of each action on both methods of marking.

QOS MARKING: BEHAVIOR

Action	802.1p (Layer 2 CoS)	DSCP (Layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) are sent out the egress interface, no 802.1p tag is added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag is explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag is preserved.	Existing DSCP tag value is preserved.	
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that is presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that is presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.

Action	802.1p (Layer 2 CoS)	DSCP (Layer 3)	Notes
Map	The setting for QoS mapping of DSCP and 802.1p tag is defined on **OBJECT | Profile Objects > QoS Marking** page.	The setting for QoS mapping of DSCP and 802.1p tag is defined on **OBJECT | Profile Objects > QoS Marking** page. An additional check box is presented to **Allow 802.1p Marking to override DSCP values**. Selecting this check box asserts the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping only occurs in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP is mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p is mapped from the DSCP tag.

Bi-directional DSCP Tag Action



HTTP access from a Web-browser on `192.168.168.100` to the Web server on `10.50.165.2` results in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to `10.50.165.2`, they bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to `192.168.168.100` (beginning with the very first SYN/ACK packet) the Access Rule (Classic Mode) or Security Action Profile (Policy Mode) tags the response packets delivered to `192.168.168.100` with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can

be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than **None**.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWall interfaces, you can begin configuring Access Rule (Classic Mode) or Security Action Profile (Policy Mode) to manage 802.1p tags.

Look at the below scenarios to understand how 802.1p and DSCP work.

- Remote Site 1: Sample Access Rule or Security Rule Configuration
- Main Site: Sample Access Rule or Security Rule Configurations

Remote Site 1: Sample Access Rule or Security Rule Configuration

The Remote Site 1 network could have two Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) configured as shown in the below table.

You can configure **QoS** on:

- Classic Mode: **OBJECT | Rules and Policies> Access Rule > Traffic Shaping**
- Policy Mode: **OBJECT | Action Profiles > Security Action Profile > Bandwidth/QoS**

Setting	Access Rule or Security Action Profile 1	Access Rule or Security Action Profile 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Primary Subnet	Main Site Subnets
Destination	Main Site Subnets	Lan Primary Subnet
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

The first Access Rule or Security Rule (governing **LAN > VPN**) would have the following effects:

- VoIP traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to Main Site Subnets would be evaluated for both DSCP and 802.1p tags.
    - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in QoS Marking Actions.
    - Sent traffic containing only an 802.1p tag (for example, CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic is 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only a DSCP tag (for example, CoS = 48) would have the DSCP value preserved on both inner and outer packets.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic is 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only both an 802.1p tag (for example, CoS = 6) and a DSCP tag (for example, CoS = 63) would give precedence to the 802.1p tag and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP would be tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

  To examine the effects of the second Access Rule (Classic Mode) or Security Action Profile (Policy Mode) (VPN > LAN), look at the Access Rule (Classic Mode) or Security Action Profile (Policy Mode) configured at main site, Main Site: Sample Access Rule or Security Rule Configurations.

Main Site: Sample Access Rule or Security Rule Configurations

Setting	Access Rule or Security Rule 1	Access Rule or Security Rule 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Subnets	Remote Site 1 Subnets
Destination	Remote Site 1 Subnets	Lan Subnets
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule or Security Rule for inbound VoIP calls. Traffic arriving at the VPN zone does not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (for example, CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (for example, CoS = 6) by the firewall at the Main Site.
- Assuming returned traffic has been 802.1p tagged (for example, CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (for example, CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (for example, CoS = 6) and DSCP tagged (for example, CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

4

Content Filter

This feature is available only in Classic Mode.

SonicOS Content Filtering Service (CFS) delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites that students and employees can access using their IT-issued computers while behind the organization's firewall.

For information about upgrading from an older version to CFS 4.0, refer to the SonicWall Content Filtering Service Upgrade Guide.

Topics:

About CFS Profile Objects

A CFS Profile Object defines the action triggered for each HTTP/HTTPS connection.

Name	Name of the CFS Profile Object; the name of the default CFS Profile Object is **CFS Default Profile**. The default object can be edited, but not deleted.
Allowed URI List	Name of the URI List Object listed in the Allowed List.
Forbidden URI List	Name of the URI List Object listed in the Forbidden List.

Block Categories	Names of all the categories blocked by the CFS Profile Object.
Passphrase Categories	Names of all the categories requiring a passphrase by this CFS Profile Object.
Confirm Categories	Names of all the categories requiring confirmation by this CFS Profile Object.
BWM Categories	Names of all the categories governed by bandwidth management by this CFS Profile Object.
Allowed Categories	Names of all the categories allowed by the CFS Profile Object.
Comments	Comments which you have added during creation of CFS Profile Object.
UUID	A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify profile objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated and read-only internal value. For more information, refer to About UUIDs for CFS Profile Objects.

About UUIDs for CFS Profile Objects

SonicOS 6.5.3 (and higher) automatically generates and binds UUIDs (Universally Unique Identifiers) for the Content Filter objects.

A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of an object and remains the same thereafter, even when the object is modified or after rebooting the firewall. The UUID is removed when the object is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

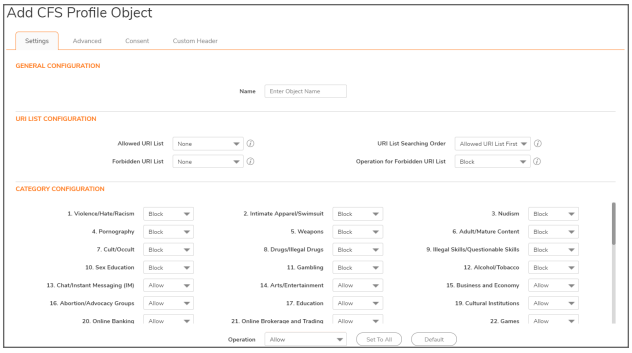
Adding CFS Profile Objects

ⓘ **NOTE:** SonicOS creates a default CFS Profile Object, **CFS Default Profile**. You can edit this CFS Profile Object, but you cannot delete it. If you do not want to use the predefined CFS profile object, you can configure a custom CFS profile object.

To add a custom CFS Profile Object:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click the **Add** icon.

   By the default, **Settings** tab displays.



3. Enter a **Name** of the CFS Profile Object.
4. Set the **URI LIST CONFIGURATION**.

   NOTE: You can set one of the options listed below for **Allowed URI List** and **Forbidden URI List**:
   - Leave the selection as **None (default)**.
   - Select the existing URI List Object.
   - Create new URI Object if you do not find the required list object in the drop-down menu. Choosing this option displays the **Add CFS URI List Object** dialog box.

     For more information about creating a URI List Object, refer to Adding URI List Objects.

   a. Select the **Allowed URI List** that contains URIs for which unrestricted access is allowed. Treat this list as a white list.

   b. Select the **Forbidden URI List** that contains URIs for which access is not allowed at all. Treat this list as a black list.

   c. Select the **URI List Searching Order** to set which URI list is searched first during filtering:
      - Allowed URI List First (default)
      - Forbidden URI List First

   d. Select the **Operation for Forbidden URI** to choose the action to be taken when a URI on the Forbidden List is encountered:

Block (default)	To block the site and display the page configured for the CFS Action Object on **OBJECT | Action Objects > Content Filter Actions** page to the user accessing the site. If you want to update the CFS Action Object, refer to Block.
Confirm	To display the confirm page configured for the CFS Action Object on **OBJECT | Action Objects > Content Filter Actions** page to the user accessing the site. The user must confirm access permission. If you want to update the CFS Action Object, refer to Confirm.

Passphrase	To display the passphrase page configured for the CFS Action Object on **OBJECT | Action Objects > Content Filter Actions** page to the user accessing the site. The user must enter a valid password to enter the site. If you want to update the CFS Action Object, refer to Passphrase.

5. Set the **Category Configuration** options in one of the following ways:
   - Select the action for each category from the drop-down menu.

     The **Category Configuration** section lists all the categories of URIs, such as Arts/Entertainment, Business, Education, Travel, Weapons, and Shopping. You can configure the action to be taken for all URIs in each category instead of individually.

     ⓘ **NOTE:** By the default, categories 1-12 and 59 are blocked, the remaining categories are allowed.

Allow	To grant access to the site.
Block	To block access to the site and displays the Block page configured on the **OBJECT | Action Objects > Content Filter Actions** page.
BWM	To regulate the site according to the CFS BWM action object configured on the **OBJECT | Action Objects > Content Filter Actions** page.
Confirm	To grant access to the site only on user confirmation with in the active time defined in Confirm page on the **OBJECT | Action Objects > Content Filter Actions** page.
Passphrase	To grant access to the site only after entering a valid password defined in Passphrase page on the **OBJECT | Action Objects > Content Filter Actions** page.

   - Set the same action for all categories according to:
     1. Select the action from the **Operation** drop-down menu.
     2. Click **Set To All**.
   - Click **Default** to reset all the categories to its default action.
6. Configure other tabs of the **Add CFS Profile Objects** as necessary.

Tab	Action
Advanced	To enable Smart Filtering and Safe Search options. For information about configuring the options on this screen, refer to Advanced Screen.
Consent	To set up web usage consent. For information about configuring the options on this screen, refer to Consent.
Custom Header	To configure Custom Header insertion. For information about configuring the options on this screen, refer to Custom Header Screen.

7. Click **Add**.

   A new CFS Profile Object is created and added to the **CFS Profile Objects** table.

Topics:

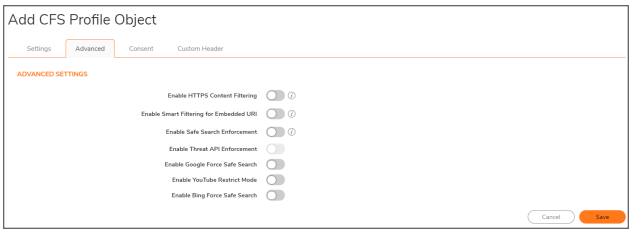
Advanced Screen

Advanced profile object helps to enable the options listed below:

- HTTPS content filtering solution to inspect the contents of secure websites in addition to regular websites.
- Threat API Enforcement.
- Safe Search to filter explicit content from search results.
  You can lock Safe Search if you want to keep Safe Search turned on and prevent users from turning it off.
- Wipe cookies.

To configure Advanced profile of the Content Filter:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Do one of the following:
   - Add a new CFS Profile Object.
     1. Click the **Add** icon.
     2. Enter a friendly profile object **Name**.
   - Edit an existing CFS Profile Object.
     Hover over an existing Profile Object and click the **Edit** icon.
3. Click the **Advanced** tab.



4. Set the **Advanced** profile object options.

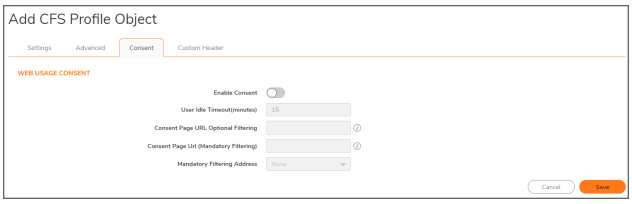
Enable HTTPS Content Filtering	To enable content filtering for HTTPS sites. This policy-based HTTPS content filtering option is available in SonicOS 6.5.3 or higher. It replaces the global HTTPS content filtering option in previous versions on the **POLICY | Security Services > Content Filter** page. ⓘ **NOTE:** When DPI-SSL client inspection is enabled and Content Filter is selected for inspection, then that inspection takes precedence and the policy-based HTTPS content filtering setting is ignored. Specifically, when the **Enable SSL Client Inspection** and **Content Filter** options are enabled on the **POLICY | DPI-SSL** page, then the **Enable HTTPS Content Filtering** option in the CFS policy is ignored. In this case, DPI-SSL will decrypt the connection and send it as plain text to CFS later for filtering. HTTPS content filtering is IP based and does not inspect the URL, but uses other methods to obtain the URL rating. When this option is enabled, CFS performs URL rating lookup in this order: • Searches the client hello for the *Server Name*, which CFS uses to obtain the URL rating. • If the Server Name is not available, searches the SSL certificate for the *Common Name*, which CFS uses to obtain the URL rating. • If neither Server Name nor Common Name is available, CFS uses the *IP address* to obtain the URL rating. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages are silently blocked.
Enable Smart Filtering for Embedded URI	To detect the embedded URL inside Google Translate (https://translate.google.com) and filter the embedded URI. ⓘ **IMPORTANT:** This feature requires enabling Client DPI-SSL with content filter. This feature takes effect only on Google Translate, which works on currently rated embedded web sites.

Enable Safe Search Enforcement	To enforce Safe Search when searching on any of the following websites: • www.yahoo.com • www.ask.com • www.dogpile.com • www.lycos.com This enforcement cannot be configured at the policy level as the function employs DNS redirection to HTTPS sites. For HTTPS sites, client DPI-SSL with content filter must be enabled.
Enable Threat API Enforcement	To enable Threat API. After SonicOS receives the initial threat list and creates a Threat URI List Object, the Threat URI List Object is referenced by **Enable Threat API Enforcement**.
Enable Google Force Safe Search	To override the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action. Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.
Enable YouTube Restrict Mode	To access YouTube in Restrict (Safe Search) mode. YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. When this feature is enabled, SonicOS rewrites the DNS response for the YouTube domain to its Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.
Enable Bing Force Safe Search	To override the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action. When this feature is enabled, SonicOS rewrites the DNS response for the Bing domain to its Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.

5. Click **Save**.

Consent

ⓘ **NOTE:** Consent only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (consent) page.



To create a web page that requires consent:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Do one of the following:
   - Add a new CFS Profile Object.
     1. Click the **Add** icon.
     2. Enter a friendly profile object **Name**.
   - Edit an existing CFS Profile Object.
     Hover over an existing Profile Object and click the **Edit** icon.
3. Click the **Consent** tab.
4. **Enable Consent** to display the Consent (Confirm) page when a user visits a site requiring consent before access.
   When this option is selected, the other options become available.
5. Set the **Consent** page options:

User Idle Timeout (minutes)	To remind users about the remaining time left to expire by displaying the **Consent** page. The minimum idle time is one minute, the maximum is 9999 minutes, and the default is 15 minutes.

Consent Page URL (optional filtering)	To enter URL of the website where a user is redirected if they go to a website requiring consent.
	The **Consent** page must:
	• Reside on a web server and be accessible as a URI by users on the network.
	• Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
	  • Unfiltered access: `<appliance's LAN IP address>/iAccept.html`
	  • Filtered access: `<appliance's LAN IP address>/iAcceptFilter.html`

Consent Page URL (mandatory filtering	To enter URL of the website where the user is redirected if they go to a website requiring mandatory filtering. The **Consent** page must: • Reside on a web server and be accessible as a URI by users on the network. • Contain a link to the `<appliance's LAN IP address>/iAcceptFilter.html` page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.
Mandatory Filtering Address	To select an Address Object that contains the configured IP addresses requiring mandatory filtering. You can select the default or custom address objects created on the **OBJECT | Match Objects > Addresses > Address Objects** page. For more information, refer to Adding Address Objects. ⓘ | **NOTE:** Make sure that **Enable Consent** is enabled to activate this feature.

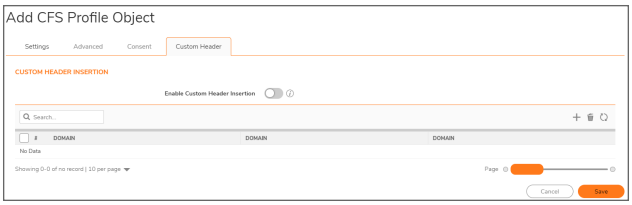
6. Click **Save**.

Custom Header Screen

From SonicOS 6.5.1 and later, you can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

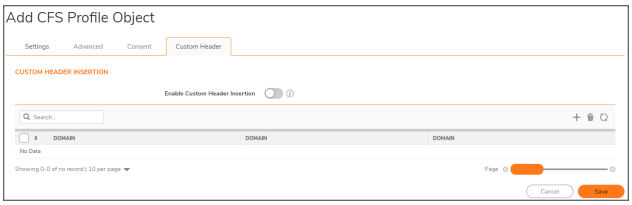
ⓘ | **IMPORTANT:** Before configuring the Custom Header, make sure that:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.



To configure a CFS custom header and enable custom header insertion:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Click the **Add** icon.
3. Click **Custom Header** tab to display the Custom Header Insertion options.
4. **Enable Custom Header Insertion** option.



5. Click **Add** icon to configure the **Domain**, **Key**, and **Value** for the custom header entry.

Domain is used to check if the host in an HTTP request is matched to an entry during packet handling. **Key** and **Value** are used to generate the right header for the entry when building runtime data for custom header insertion.

Make sure that the Domain follows the conditions listed below:

- Each domain name can contain up to 16 tokens separated by periods (.).
- The domain name cannot start or end with separators.
- Each token can contain up to 128 printable ASCII characters.
- Tokens in a domain name can only contain the characters: *0-9a-zA-z$-_+!'(),*.
- IPv4/IPv6 addresses can be defined as a domain name, e.g. [2001:2002:2003::2005:2006].

6. Click **Save**.

Editing CFS Profile Objects

ⓘ | **NOTE:** You can edit the default profile also but you cannot modify Name of it.

To edit a CFS Profile object:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Hover over the CFS Profile object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding CFS Profile Objects.
4. Click **Save**.

Deleting CFS Profile Objects

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete custom CFS Profile Objects:

1. Navigate to **OBJECT | Profile Objects > Content Filter**.
2. Do one of the following:
   - Hover over the Profile object to be deleted and click the **Delete** icon.
   - Select check boxes of the Profile objects to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom CFS profile objects are selected.
3. Click **Confirm**.

Applying Content Filter Profile Objects

NOTE: Make sure that **Enable Content Filtering Service** option is enabled on the **POLICY | Security Services > Content Filter** page to enable the service.

Once the Content Filter Profiles are configured, you can apply them in Content Filter policies on the **POLICY | Rule and Policies > Content Filter Rules** page. For more information, refer to Content Filter Rules section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

5

DHCP Option

A SonicWall network security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. **NETWORK | System > DHCP Server** includes settings for configuring the appliance's DHCP server, Lease Scopes, and DHCP Leases.

The SonicWall DHCP Server provides support for DHCP Options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP Options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. For more information on RFC-Defined DHCP Option Numbers, refer to:

- IPv4 Options: RFC-Defined DHCPV4 Option Numbers
- IPv6 Options: RFC-Defined DHCPV6 Option Numbers

From **DHCP Option** page, you can:

- Filter the table data with a specific string
- Add, modify, and delete custom IPv4 and IPv6 profiles
- Clone from an exiting one to create a new one
- Refresh and sort the table columns data to identify the specific results

Topics:

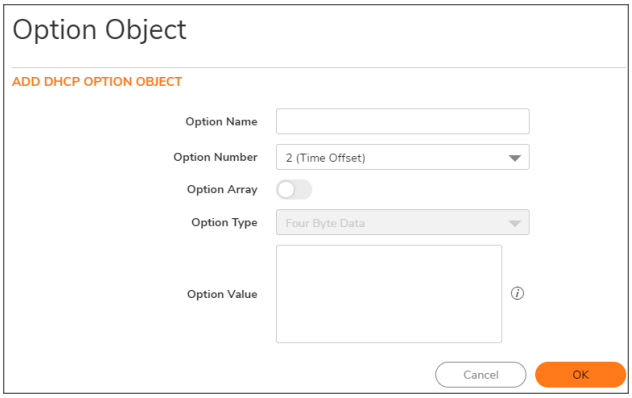
Prerequisites

Make sure that **Enable DHCPv4 Server** and **Enable DHCPv6 Server** are enabled under IPv4 and IPv6 respectively on **NETWORK | System > DHCP Server > DHCP Server Settings** page.

Adding DHCP Option Objects

To add DHCP option object:

1. Navigate to **OBJECT | Profile Objects > DHCP Option**.
2. Click **IPv4** or **IPv6** option under which you want to create the option object.
3. Click the **Add** icon.



4. Enter an **Option Name** for the option object.
5. Select the **Option Number** that corresponds to your DHCP option.

   For a list of option numbers, names, and descriptions, refer to:

   - IPv4 Options: RFC-Defined DHCPV4 Option Numbers
   - IPv6 Options: RFC-Defined DHCPV6 Option Numbers

6. Do one of the following:

   - Enter the **Option Value** if only one **Option Type** is available for the selected **Option Number**.

     For example, for **Option Number 2 (Time Offset)**, only one **Option Type** is available and the **Option Array** option is unavailable.

   - If multiple options are available for the selected **Option Number**:

     For example, for **77 (User Class Information)**, you can select the **Option Type** from the drop-down menu such as **IP Address**, **Two-Byte Data**, **String**, **Boolean**, and so on.

     1. Select the **Option Type**.
     2. Enter the **Option Value**, for example, an IP address.

        ⓘ **NOTE:** Enable the **Option Array** to enter multiple values in the **Option Value** field separated by a semi-colon (;).

7. Click **Save**.
8. Click **Cancel** to go back to DHCP Option page.

   The option object is created and displayed in the respective **Option Objects** table.

DHCPV4 OPTION OBJECTS TABLE

DHCPV6 OPTION OBJECTS TABLE

RFC-Defined DHCPV4 Option Numbers

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Routers	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string, such as (Server Unicast)
13	Boot File Size	Size of boot file in 512-byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table

Option Number	Name	Description
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload **sname** or **file**
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier

Option Number	Name	Description
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91- 92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol

Option Number	Name	Description
96	Undefined	N/A
97	UUID/GUID-based Client Identifier	UUID/GUID-based client identifier
98	Open Group's User Authentication	Open group's user authentication
99 - 108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110 - 111	Undefined	N/A
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126 - 127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136 - 149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151 - 174	Undefined	N/A

Option Number	Name	Description
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178 - 207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212 - 219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222 - 223	Undefined	N/A
224 - 257	Private Use	Private use

RFC-Defined DHCPV6 Option Numbers

Option Number	Name	Description
12	Server Unicast	Hostname string, such as (Server Unicast)
21	SIP Servers Domain Name List	Enables listing of SIP Servers domain names
22	SIP Servers IPv6 Address List	Enables listing of SIP Servers IPv6 Addresses
23	DNS Recursive Name Server	Enables listing of DNS Recursive Name servers
24	Domain Search List	Enables listing of domain names for searching
27	Network Information Service (NIS) Servers	Enables listing of Network Information Service (NIS) servers
28	Network Information Service V2 (NIS+) Servers	Enables listing of Network Information Service V2 (NIS+) servers
29	Network Information Service (NIS) Domain Name	Enables listing of Network Information Service (NIS) domain names
30	Network Information Service V2 (NIS+) Domain Name	Enables listing of Network Information Service V2 (NIS+) domain names
31	Simple Network Time Protocol (SNTP) Servers	Enables listing of Simple Network Time Protocol (SNTP) servers

Option Number	Name	Description
32	Information Refresh Time	Information refresh time

Editing DHCP Option Objects

To edit DHCP option object:

1. Navigate to **OBJECT | Profile Objects > DHCP Option**.
2. Click **IPv4** or **IPv6** option under which you want to delete the option object.
3. Hover over the DHCP Option Object to be edited and click the **Edit** icon.
4. Make the necessary changes. For more information, refer to Configuring DHCP Option Objects.
5. Click **Save**.

Deleting DHCP Option Objects

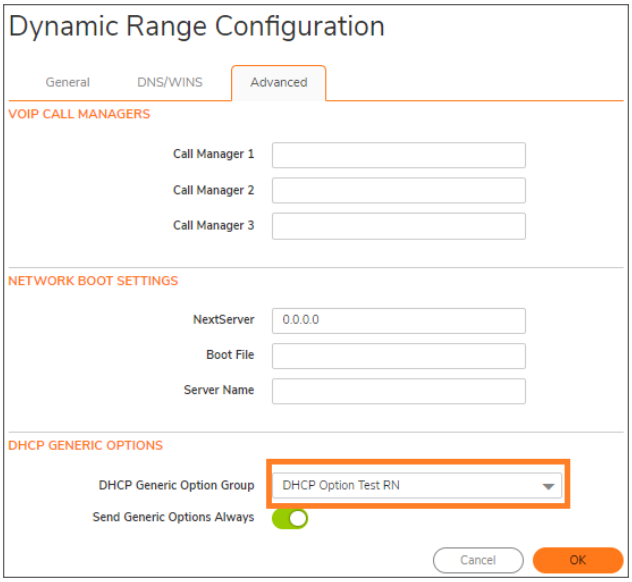
ⓘ | **NOTE:** You cannot delete an item if it is in use by DHCP Server.

To delete DHCP option object:

1. Navigate to **OBJECT | Profile Objects > DHCP Option**.
2. Click **IPv4** or **IPv6** option under which you want to delete the option object.
3. Do one of the following:
   - Hover over the DHCP Option to be delete and click the **Delete** icon.
   - Select check boxes of the option objects to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header to delete all option objects and click the **Delete** icon on top of the table.
4. Click **OK**.

Applying DHCP Option Objects

Once the DHCP Option Objects are created, you can apply them in configuring **DHCP Server** on the **NETWORK | System > DHCP Server > DHCP Server Lease Scopes** page. For more information, refer to **DHCP Server** section in SonicOS 7.0 System Administration Guide.



6

Block Page

Block Page profile object feature is available only in Policy Mode.

You can configure a default message that displays when user attempts to access a blocked page with detailed information, such as the reason for IP address blockage, IP address, and the country from which it was detected. You can also create a block page with a custom message and include a custom logo.

SonicOS creates the **Default Block Page**. You can use the default page or create a new ones based on your requirements.

From the **Block Page**, you can:

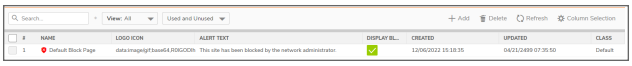
- Filter the table data
- Add, modify, and delete block pages
- Clone from an exiting pages to create a new page
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

Topics:

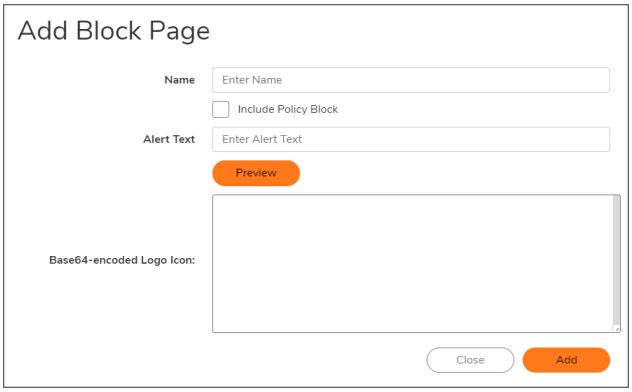
Adding Custom Block Pages

To configure a custom block page message:

1. Navigate to **OBJECT | Profile Objects > Block Page**.



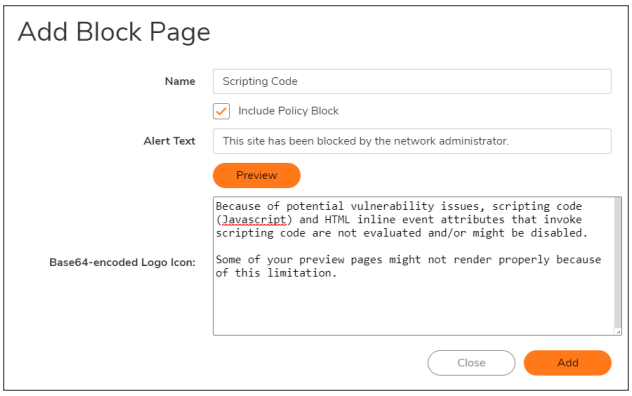
2. Click the **Add** icon.



> ⓘ **NOTE:** Ensure the **Include Policy Block** option is selected. When selected, this option shows block details such as reason for the block, IP address, and country. When disabled, no information is displayed.

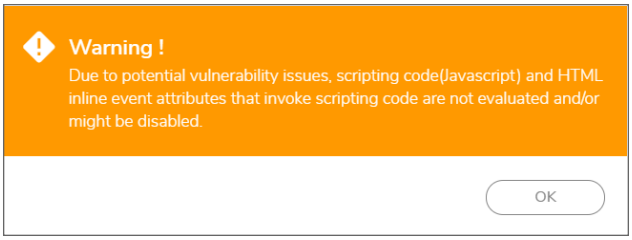
3. Do one of the following:
   - Enter a message to be displayed in the **Alert Text** field, such as `This site has been blocked by the network administrator.`
   - Specify a custom message to be displayed in the **Base64-encoded Logo Icon** page in the text field. Your message can be up to 100 characters long.

5. Specify a Base 64-encoded GIF icon n the **Base64-encoded Logo Icon** field if you want to replace the default SonicWall logo.



ⓘ | **NOTE:** Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

6. Click **Preview** to display the preview of your customized message and logo (or the default message and logo).



7. Click **OK**.
   The **Web Site Blocked** message displays.

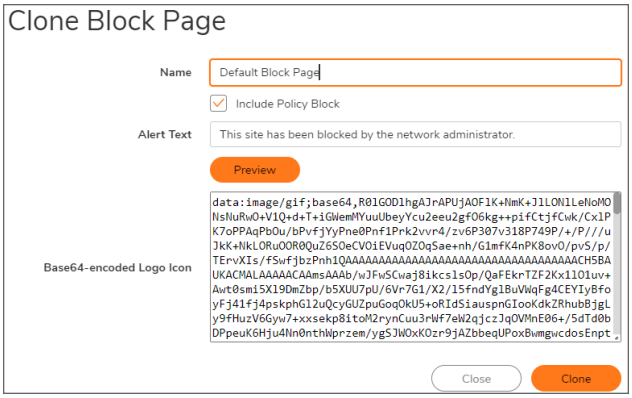
8. Close the **Web Site Blocked** message.
9. Click **Add**.
   New block page is added to the table.
10. Click **Close** to go back to **Block Page**.

Cloning Block Page

ⓘ | **NOTE:** **Clone** option helps to create a new block page with the help of an existing block page.

To clone an existing custom block page message:

1. Navigate to **OBJECT | Profile Objects > Block Page**.
2. Hover over the Block Page you want to clone and click the **Clone** icon.

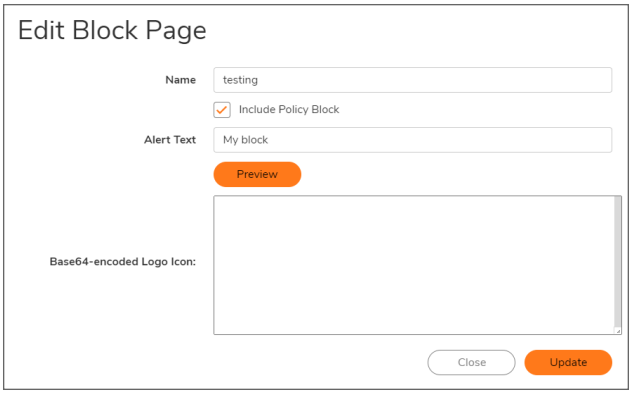


3. Make the necessary changes to the **Clone Block Page** form. For more information, refer to Adding Custom Block Pages.
4. Click **Clone**.
   New block page is added to the table.
5. Click **Close** to go back to **Block Page**.

Editing Block Pages

To edit a custom block page message:

1. Navigate to **OBJECT | Profile Objects > Block Page**.
2. Hover over the Block Page to be edited and click the **Edit** icon.



2. Make the necessary changes.
   For more information, refer to Adding Custom Block Pages.

3. Click **Update**.
4. Click **Close** to go back to **Block Page**.

Deleting Block Pages

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom block page:

1. Navigate to **OBJECT | Profile Objects > Block Page**.
2. Hover over the custom block page to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the Delete dialog box.

To delete multiple or all custom block pages:

1. Navigate to **OBJECT | Profile Objects > Block Page**.
2. Do one of the following:
   a. Select check boxes of the block pages to be deleted.
   b. Select the check box in the table header to select all custom block pages.
3. Click the **Delete** icon on top of the table.
4. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.

Applying Block Pages

Once the Block Pages are configured, you can apply them in configuring **Security Action Profiles** on **OBJECT | Action Profiles > Security Action Profile** page. For more information, refer to Block Page and Logging.

7

Anti-Spyware

Anti-Spyware Profiles are available only in Policy Mode.

An Anti-Spyware is a spyware protection, designed to detect, prevent, and remove spyware and adware infections. An Anti-Spyware actively scans inbound and outbound traffic from e-mails, websites, and downloaded files to block spyware from entering the system.

The detection works based on a Security Policy defined on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

From the **Anti-Spyware** page, you can:

- View all SonicWall spyware signatures from **Anti-Spyware Objects** tab.
- Enable or disable SonicWall spyware signatures from **Anti-Spyware Objects** tab.
- Create category profiles on a signature by signature basis to configure the handling of those signatures from **Anti-Spyware Profiles**.

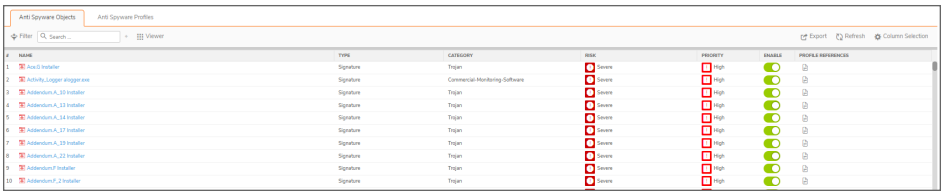
  Anti-Spyware Profiles are signatures grouped together based on attributes such as types of attack.
- Clone from an exiting one to create a new one
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

Topics:

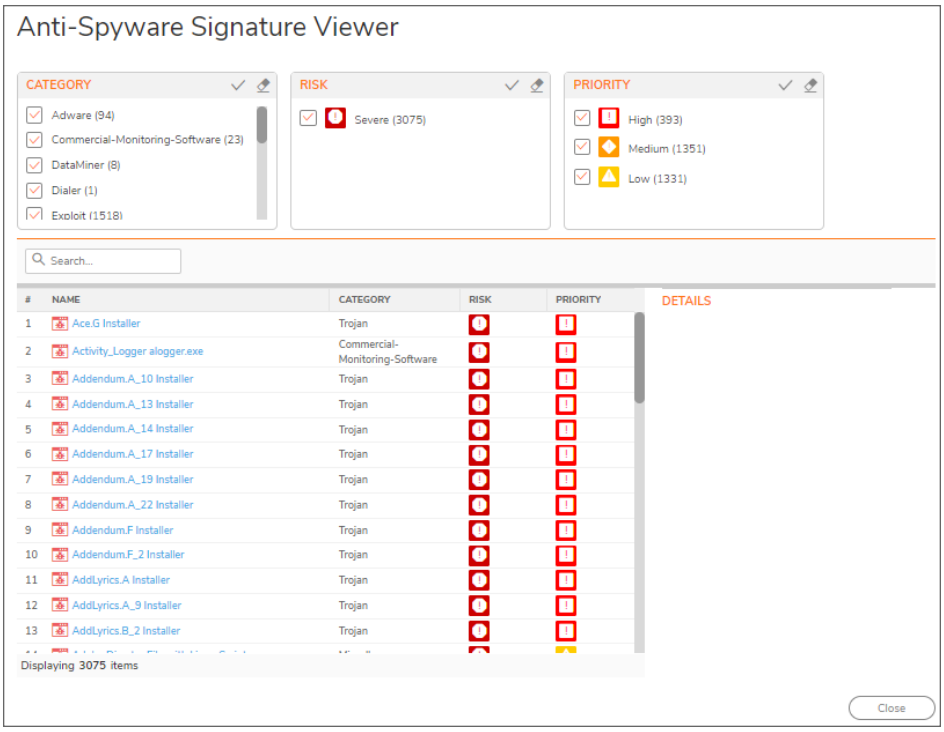
Viewing Anti-Spyware Objects

To view the Anti-Spyware Objects:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware**.



2. Click the **Viewer** to set the filters and view the results.
   Select the filters to narrow down the results being displayed based on **Category**, **Risk**, and **Priority**.
   Results of your filtering appear in the lower portion of the **Viewer**.

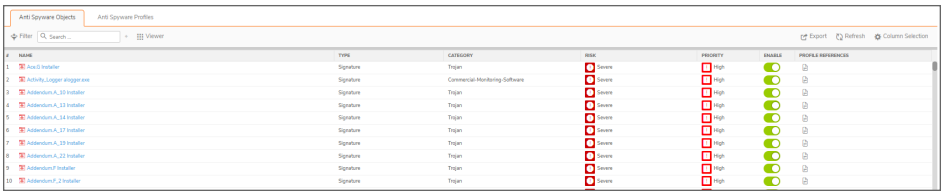


Enabling or Disabling Anti-Spyware Objects

ⓘ **NOTE:** By the default, all the Anti-Spyware signatures are enabled under the Anti-Spyware Objects. If the signatures are disabled in the Anti-Spyware Objects table, those are not matched.

To enable or disable the Anti-Spyware Objects:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware**.



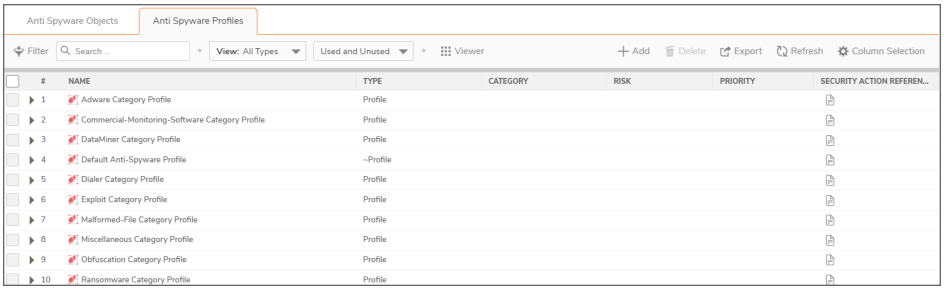
2. Enable or disable the signature under the **Enable** column.

Adding Anti-Spyware Profiles

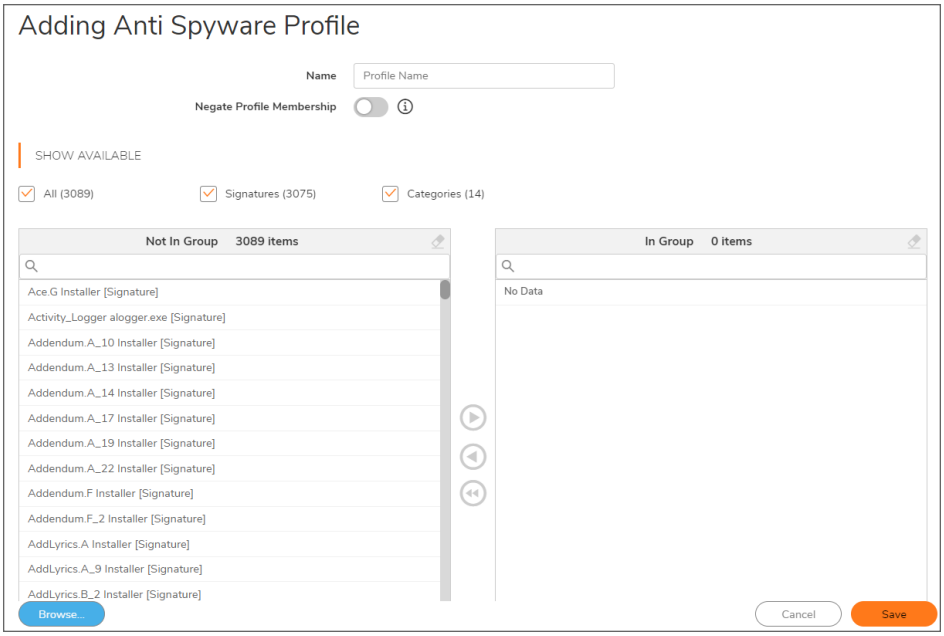
Create Anti-Spyware Profiles to enforce rules and actions imposed through your Security Rule Actions. Filter your results with the **Anti-Spyware Profiles Viewer**.

To add an Anti-Spyware Profiles:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware > Anti-Spyware Profiles**.



2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.
4. Enable **Negate Profile Membership**.
   A negate directive includes all signatures into a profile which is not in the list of selected signatures.
5. Select the required items from the **Not in Group** list.
   Press the **Ctrl** or **Shift** key to select multiple items.
6. Click the right arrow to add the selected items to the group.
7. Click **Browse** if you want to select the applications from the **Application Selector** window.
8. Click Plus (+) icon of applications to be included and click **Select**.
9. Click **Save**.
10. Click **Cancel** to go back to Anti-Spyware Profiles page.

Editing Anti-Spyware Profiles

ⓘ | **NOTE:** You can edit only custom profiles.

To edit an Anti-Spyware Profile:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware > Anti-Spyware Profiles**.
2. Set the **View** drop-down menu to **Custom**.
3. Hover over the profile to be edited and click the **Edit** icon.
4. Make the necessary changes.
   For more information, refer to Adding Anti-Spyware Profiles.
5. Click **Save**.

Cloning Anti-Spyware Profiles

ⓘ | **NOTE:** You can clone from custom profiles only.

To clone an existing Anti-Spyware Profile:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware > Anti-Spyware Profiles**.
2. Hover over the custom profile you want to clone and click the **Clone** icon.
   This creates a duplicate of the page, which allows you to create a new profile with the similar content.
3. Make the necessary changes. For more information, refer to Adding Anti-Spyware Profiles.
4. Click **Save**.

Deleting Anti-Spyware Profiles

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom Anti-Spyware Profile:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware > Anti-Spyware Profiles**.
2. Hover over the profile to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom Anti-Spyware Profiles:

1. Navigate to **OBJECT | Profile Objects > Anti-Spyware > Anti-Spyware Profiles**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Anti-Spyware Profiles

Once the Anti-Spyware Profiles are created, you can apply them in configuring Anti-Spyware Security Action Profiles on **OBJECT | Action Profiles > Security Action Profile** page. These Security Action Profiles can be used to configure a security policy on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

8

Gateway Anti-Virus

Gateway Anti-Virus Profiles are available only in Policy Mode.

Gateway Anti-Virus is a network security appliance feature that blocks potential threats before reaching the network.

The detection works based on a Security Policy defined on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

From the **Gateway Anti-Virus** page, you can:

- View all SonicWall virus signatures from **Gateway Anti-Virus Objects** tab.
- Create category profiles on a signature by signature basis to configure the handling of those signatures from **Gateway Anti-Virus Profiles**.

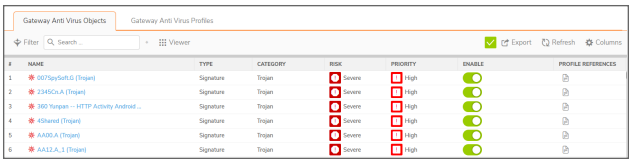
  Gateway Anti-Virus Profiles are signatures grouped together based on attributes such as types of attack.
- Clone from an exiting one to create a new one
- Export the table information into CSV file
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

Topics:

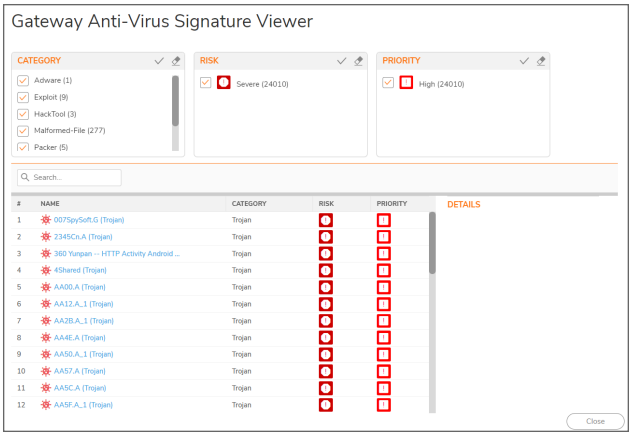
Viewing Gateway Anti-Virus Objects

To view the Gateway Anti-Virus Objects:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus**.



2. Click the **Viewer** to set the filters and view the results.
   Select the filters to narrow down the results being displayed based on **Category**, **Risk**, and **Priority**.
   Results of your filtering appear in the lower portion of the **Viewer**.

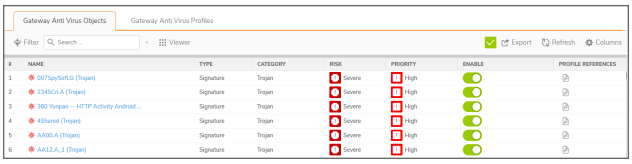


Enabling or Disabling Gateway Anti-Virus Objects

ⓘ **NOTE:** By the default, all the Gateway Anti-Virus signatures are enabled under the Gateway Anti-Virus Objects. If the signatures are disabled in the Gateway Anti-Virus Objects table, those are not matched.

To enable or disable the Gateway Anti-Virus Objects:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus**.



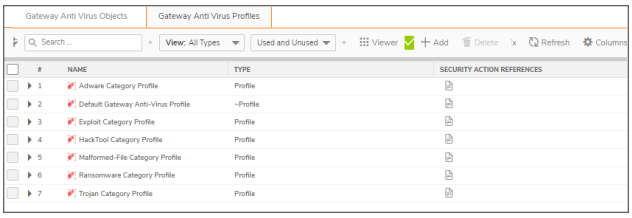
2. Enable or disable the signature under the **Enable** column.

Adding Gateway Anti-Virus Profiles

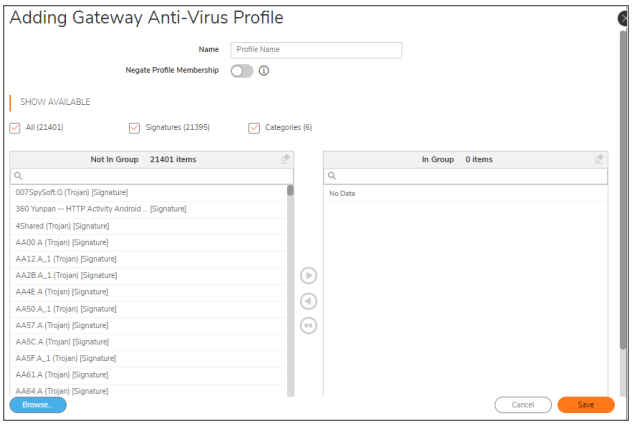
Create Gateway Anti-Virus Profile Objects to enforce rules and actions imposed through your Security Rule Actions. Filter your results with the **Gateway Anti-Virus Profiles Viewer**.

To add aGateway Anti-Virus Profile Object:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus > Gateway Anti-Virus Profiles**.



2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.
4. Enable **Negate Profile Membership**.
   A negate directive includes all signatures into a profile which is not in the list of selected signatures.
5. Select the required items from the **Not in Group** list.
   Press the **Ctrl** or **Shift** key to select multiple items.
6. Click the right arrow to add the selected items to the group.
7. Click **Browse** if you want to select the applications from the **Application Selector** window.
8. Click Plus (+) icon of applications to be included and click **Select**.
9. Click **Save**.
10. Click **Cancel** to go back to Gateway Anti-Virus Profiles page.

Cloning Gateway Anti-Virus Profiles

ⓘ | **NOTE:** You can clone from custom profiles only.

To clone from an existing Gateway Anti-Virus Profile:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus > Gateway Anti-Virus Profiles**.
2. Hover over the custom profile you want to clone and click the **Clone** icon.
   This creates a duplicate of the page, which allows you to create a new profile with the similar content.
3. Make the necessary changes.
   For more information, refer to Adding Gateway Anti-Virus Profiles.
4. Click **Save**.

Editing Gateway Anti-Virus Profiles

ⓘ | **NOTE:** You can edit only custom profiles.

To edit an existing Gateway Anti-Virus Profile:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus > Gateway Anti-Virus Profiles**.
2. Hover over the profile to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Gateway Anti-Virus Profiles.
4. Click **Save**.

Deleting Gateway Anti-Virus Profiles

ⓘ | **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete custom Gateway Anti-Virus Profiles:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus > Gateway Anti-Virus Profiles**.
2. Hover over the profile to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom Gateway Anti-Virus Profiles:

1. Navigate to **OBJECT | Profile Objects > Gateway Anti-Virus > Gateway Anti-Virus Profiles**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.
   b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status.
      Operation gets failed if one of the items is in use by rule.

Applying Gateway Anti-Virus Profiles

Once the Gateway Anti-Virus Profiles are created, you can apply them in configuring Anti-Virus Security Action Profiles on **OBJECT | Action Profiles > Security Action Profile** page. These Security Action Profiles can be used to configure a security policy on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

9

Log and Alerts

Log and Alerts feature is available only in Policy Mode.

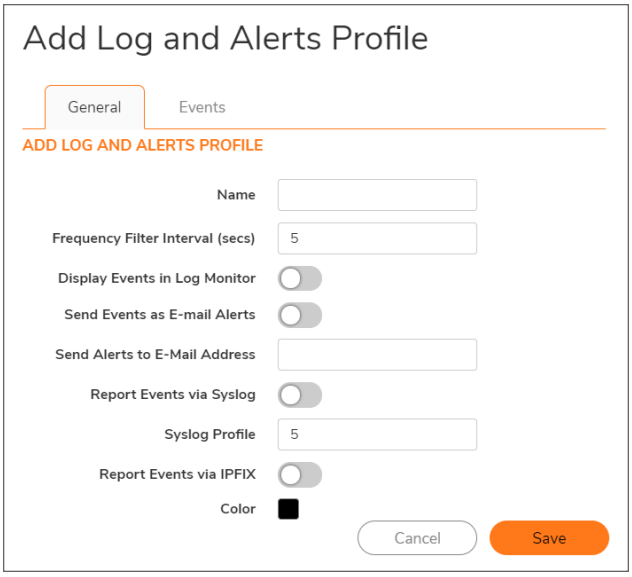
From **Log and Alerts**, profiles can be configured to specify the method and frequency of message notification when monitored events occur in the system. The Log and Alert Profile settings take effect as a rule action when network traffic matches a Security Rule.

Topics:

Adding Log and Alerts Profiles

To add a Log and Alert Profile:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Click the **Add** icon.
   By the default, **General** tab opens.



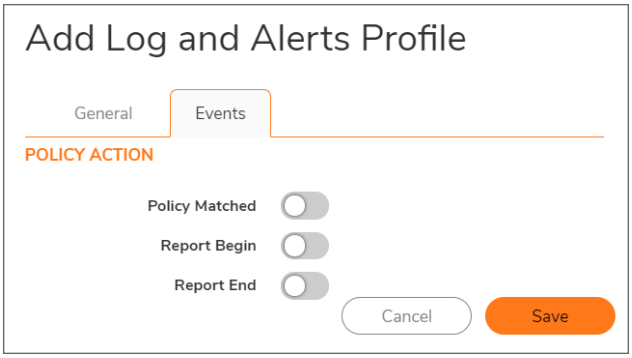
3. Enter a **Name** for Log and Alerts Profile.
4. Set the **Frequency Filter Interval (secs)** between reports.

   TIP:
   - The Frequency Interval (secs) controls how many seconds to countdown from before logging another occurrence of the same Event Message ID. The range of interval is 0 to 86400 seconds.
   - In general, most messages seen on Log Monitor are logged at one occurrence for every 60 seconds. Most Syslog messages are generated at one occurrence every 60 seconds. Most e-mail alerts are sent at one occurrence every 900 seconds.
   - To allow all occurrences with no filtering, a value of zero should be configured.
5. Set the **General** options of the Log and Alerts Profile.

Display Events in Log Monitor	To display the log events in the Log Monitor.

Send Events as E-mail Alerts	To send events as e-mail alerts. When this option is enabled, enter the e-mail address in the **Send Alerts to E-Mail Address** field to send the events.
Report Events via Syslog	To report events through Syslog. The Syslog Profile can be found in **DEVICE | Log > Syslog > Syslog Servers** tab. When this option is enabled, enter the **Sylog Profile** you would like to use.
Report Events via IPFIX	To report events by way of IPFIX.

6. Click the **Color** box and set the specific color for Log Monitor display.
7. Click the **Events** tab.



8. Enable the **Events** options of the Log and Alerts Profile.

Policy Matched	When a security rule is matched, the log message id=1640 **Policy Matched** is originated from the rule lookup when a new flow is encountered.
Report Begin	When a connection associated with a rule is opened or started, this controls whether the log message id=98 **Connection Opened** is originated. If disabled, there will be no Connection Opened log message generated for the packets or flow associated with this log profile.
Report End	This controls whether the closing or ending of the connection is reported using log message ids (97 **Syslog Website Accessed** or 537 **Connection Closed**). These two messages (97, 537) are essentially the same except for extra Web Stream information included in (97) because it is generated for Web Stream types of connections that have non-zero traffic data. Non-Web Stream connections use (537). An exception for Web Stream connection that has zero traffic data will also use (537) since there will be no extra Web Stream information inspected.

9. Click **Save**.
10. Click **Close** to go back to **Log and Alerts** page.

Editing Log and Alert Profiles

ⓘ | **NOTE:** You can edit only custom profiles.

To edit a Log and Alert Profile:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Hover over the profile to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Log and Alerts Profiles.
4. Click **Save**.

Deleting Log and Alert Profiles

ⓘ | **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom log and alert profile:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Hover over the custom profile to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom log and alert profiles:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Do one of the following:
   a. Select check boxes of the block pages to be deleted.
   b. Select the check box in the table header to select all custom block pages.
3. Click the **Delete Selected** icon on top of the table.
4. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.

Applying Log Alerts Profiles

Once the profiles are configured, they can be selected in Security Action Profiles on **OBJECT | Action Profiles > Security Action Profile > Block Page and Logging** page under **LOG AND ALERTS** group. For more information, refer to Block Page and Logging.

10

Intrusion Prevention

Intrusion Prevention Profiles are available only in Policy Mode.

Intrusion Prevention Service (IPS) delivers a configurable, high performance Deep Packet Inspection (DPI) engine for extended protection of key network services such as Web, E-mail, file transfer, Windows services, and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and back-door exploits. The extensible signature language used in SonicWall's DPI engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS off-loads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

The detection works based on a Security Policy defined on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

From the **Intrusion Prevention**, you can:

- View all SonicWall threat signatures from **Intrusion Prevention Objects** tab.
- Create category profiles on a signature by signature basis to configure the handling of those signatures from **Intrusion Prevention Profiles** which can be used in configuring Intrusion Prevention Security Rule Actions on **OBJECT | Action Profiles > Security Action Profile** page. These Security Action Profiles can be applied in defining Security Policy on **POLICY | Rules and Policies > Security Policy** page.

  Intrusion Prevention Profiles are signatures grouped together based on attributes such as types of attack.
- Clone from an exiting one to create a new one
- Refresh and sort the table columns data to identify the specific results
- Customize columns to show or hide the table columns, and save the filter preferences for next time log in

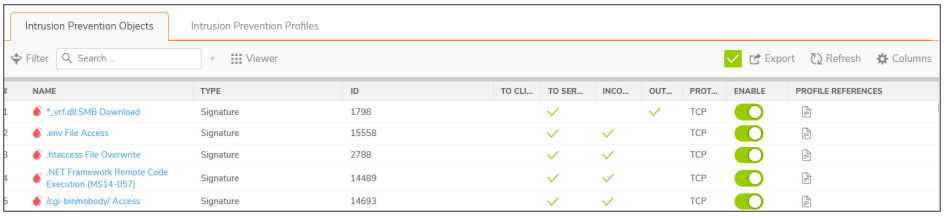
Topics:

- Viewing Intrusion Prevention Objects
- Enabling or Disabling Intrusion Prevention Objects
- Adding Intrusion Prevention Profiles
- Editing Intrusion Prevention Profiles
- Cloning Intrusion Prevention Profiles
- Deleting Intrusion Prevention Profiles
- Applying Intrusion Prevention Profiles

Viewing Intrusion Prevention Objects

To view the Intrusion Prevention Objects:

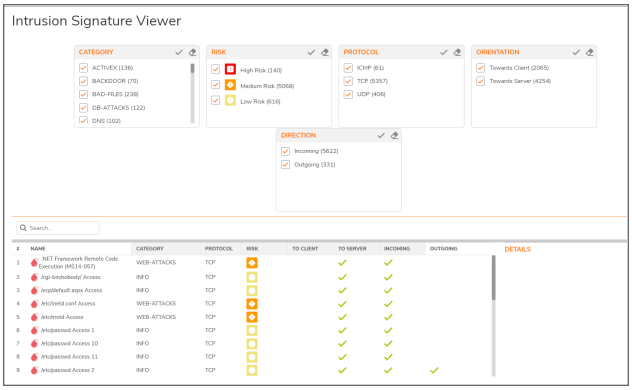
1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention**.



2. Click the **Viewer** to set the filters and view the results.

   Select the filters to narrow down the results being displayed based on **Category**, **Risk Level**, **Protocol**, **Orientation**, and **Direction**.

   Results of your filtering appear in the lower portion of the **Viewer**.

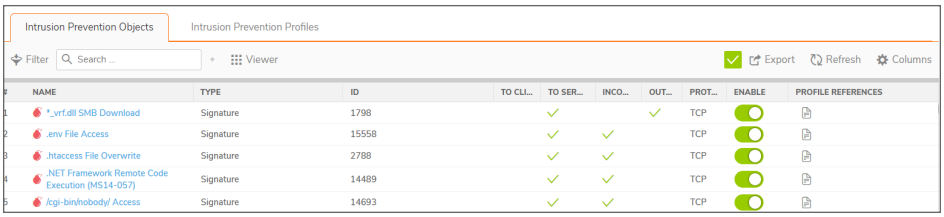


Enabling or Disabling Intrusion Prevention Objects

ⓘ **NOTE:** By the default, all the Intrusion Prevention threat signatures are enabled under the Intrusion Prevention Objects. If the signatures are disabled in the Intrusion Prevention Objects table, those are not matched.

To enable or disable the Intrusion Prevention Objects:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention**.



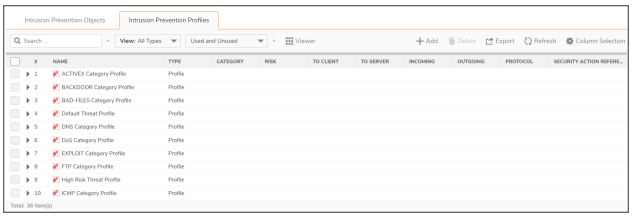
2. Enable or disable the signature under the **Enable** column.

Adding Intrusion Prevention Profiles

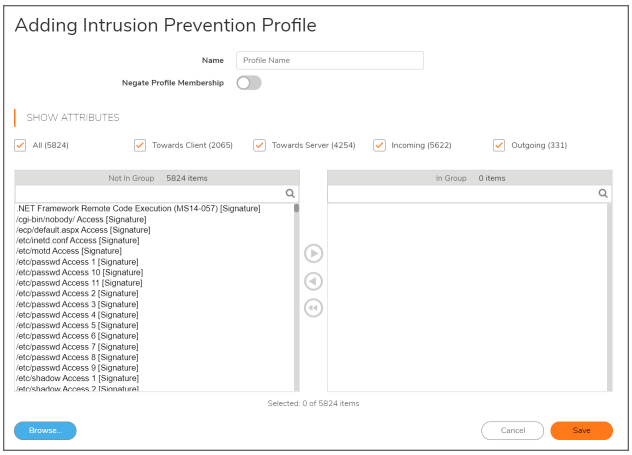
Create Intrusion Prevention Profiles to enforce rules and actions imposed through your Security Rule Actions. Filter your results with the **Intrusion Prevention Profiles Viewer**.

To add an Intrusion Prevention Profile:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles**.



2. Click the **Add** icon.



3. Enter a descriptive and unique **Name** for the group.
4. Enable **Negate Profile Membership**.
   A negate directive includes all signatures into a profile which is not in the list of selected signatures.
5. Select the required items from the **Not in Group** list.
   Press the **Ctrl** or **Shift** key to select multiple items.
6. Click the right arrow to add the selected items to the group.
7. Click **Browse** if you want to select the applications from the **Application Selector** window.
8. Click Plus (+) icon of applications to be included and click **Select**.
9. Click **Save**.

Editing Intrusion Prevention Profiles

ⓘ | **NOTE:** You can edit only custom profiles.

To edit an existing Intrusion Prevention Profile:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles**.
2. Hover over the profile to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Intrusion Prevention Profiles.
4. Click **Save**.

Cloning Intrusion Prevention Profiles

ⓘ | **NOTE:** You can clone from custom profiles only.

To clone from an existing Intrusion Prevention Profile:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles**.
2. Hover over the custom profile you want to clone and click the **Clone** icon.
   This creates a duplicate of the profile, which allows you to create a new profile with the similar content.
3. Make the necessary changes.
   For more information, refer to Adding Intrusion Prevention Profiles.
4. Click **Save**.

Deleting Intrusion Prevention Profiles

ⓘ | **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom Intrusion Prevention Profile:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles**.
2. Hover over the profile to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom Intrusion Prevention Profiles:

1. Navigate to **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Do one of the following:
   a. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.
      Deletes only unused items and shows the status of each item.

b. Click **Bulk Delete** to delete all of the selected items in one attempt and view the final status. Operation gets failed if one of the items is in use by rule.

Applying Intrusion Prevention Profiles

Once the Intrusion Prevention Profiles are created, you can apply them in configuring Intrusion Prevention Security Action Profiles on **OBJECT | Action Profiles > Security Action Profile** page. These Security Action Profiles can be used to configure a security policy on **POLICY | Rules and Policies > Security Policy** page. For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

11

AWS

Before setting up AWS objects or groups, make sure that the firewall is configured with the AWS credentials. You can configure the firewall with AWS on **NETWORK | System > AWS Configuration** page and validate the settings using the **Test Configuration** before proceeding. For more information, refer to *Configuring AWS Credentials* in the *SonicOS System Setup* administration documentation.

You can find the configuration link on the **OBJECT | Profile Objects > AWS** page also if AWS is not yet configured. Click the link which directs you to the **NETWORK | System > AWS Configuration** page.

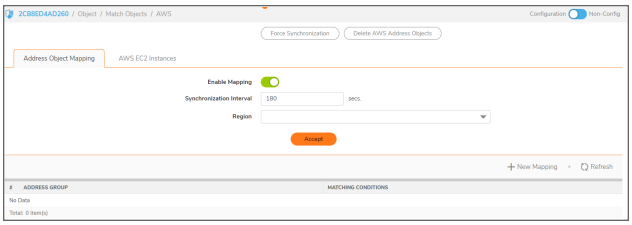
Topics:

AWS Objects

The **AWS** page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with address objects and address groups configured on the firewall.

New address objects are created for Instance IP addresses, address groups for all addresses of an Instance and those Instance address groups can be added to existing address groups. Those objects, as with any other address objects and address groups, can then be used in firewall policies and features to permit or block access, route traffic and so on.

The **OBJECT | Profile Objects > AWS** page allows SonicOS administrator to specify sets of EC2 Instance properties. If any of the Instances in one of the monitored regions matches a set of properties, address objects and address groups are created so that, effectively an address group representing the Instance is added to the custom, pre-existing address group specified in the relevant mapping. This address group can be used in firewall policies and, thus, those policies can shape the interaction with EC2 Instances running on AWS.



Topics:

- About Address Object Mapping with AWS
- Viewing Instance Properties in SonicOS
- Creating a New Address Object Mapping
- Enable Mapping
- Configuring Synchronization
- Configuring Regions to Monitor
- Verifying AWS Address Objects and Groups

About Address Object Mapping with AWS

EC2 Instances are virtual machines (VMs) running on AWS. Each instance can be one of number of different available types, depending on the resources required for that instance by the customer. The virtual machine is an instance of a particular Amazon Machine Image (AMI), essentially a template and a specification for VMs that are created from it. All EC2 Instances have a number of properties including:

- Instance type
- AMI used in their creation
- Running state
- ID used for identification
- ID of the Virtual Private Cloud (VPC) where the Instance is located
- A set of user defined tags

You can use any or all of those properties to map matching Instances to address groups that a SonicOS administrator has previously configured on the firewall. Those address groups can be used in Route, VPN and Firewall Policies which can affect how the firewall interacts with AWS hosted machines.

In order to map EC2 Instances to firewall address groups, the Administrator configures any number of mappings between sets of instance properties and pre-existing address groups. If an EC2 Instance, in any of the monitored AWS Regions, matches a set of specified properties, one or more address objects and a single address group are created to represent that Instance and that address group is added to the target address group of the relevant mapping.

EC2 Instances can have multiple private and public IP addresses depending on the number of virtual network interfaces and the use of Elastic IP Addresses. When an Instance matches the properties specified in a mapping, address objects are created for each of its IP addresses, both public and private. Those address objects are then added into one address group which represents the EC2 Instance as a whole. It is that *Instance address group* that is then added to the mapping's target address group, an existing address group used in the configuration of

the various firewall policies. Any one EC2 Instance may match the criteria of more than one mapping, in which case the Instance address group is added to more than one target address group. There are no limits.

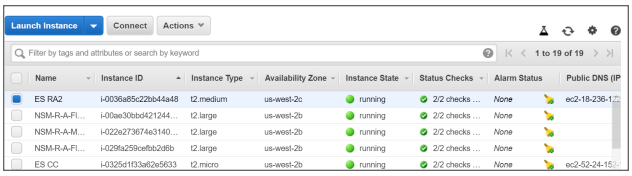
Topics:

Tagging an EC2 Instance on AWS

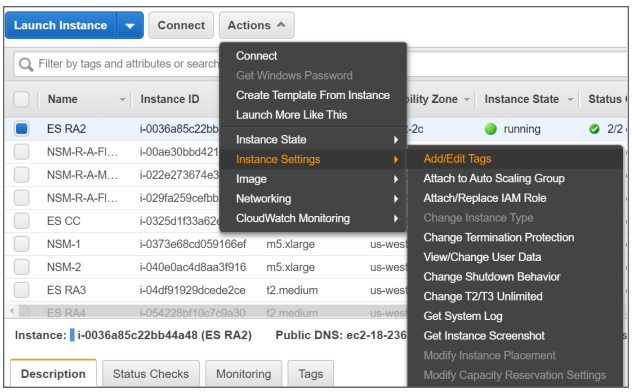
You can tag an EC2 Instance in multiple ways. This section describes the steps to tag an EC2 Instance manually.

To manually add a tag to an existing EC2 Instance:

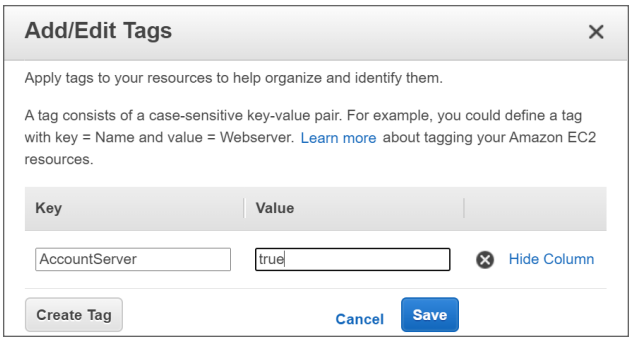
1. On the AWS Console, navigate to the EC2 Dashboard and turn to the Instances page.
2. Select check box of the Instance that you want to tag.



3. Click **Actions > Instance Settings > Add/Edit Tags**.

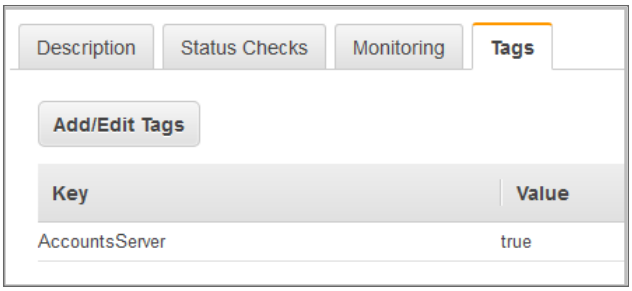


4. Enter descriptive values in the **Key** and **Value** fields.
5. Click **Save** to tag the Instance with entered key and value.



6. Verify the tag on the Instances page under the EC2 Dashboard.

   With the Instance still selected, click the **Tags** tab to view the associated tags in the panel at the bottom of the page. This provides confirmation that the EC2 Instance has been tagged.

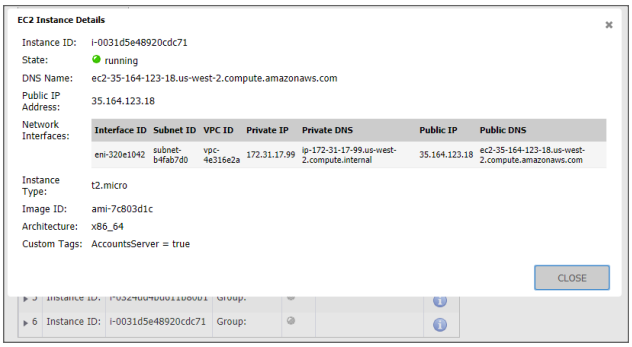


   You can now use that tag while defining address object mappings in the SonicOS management interface.

Viewing Instance Properties in SonicOS

The **OBJECT | Profile Objects > AWS** page provides a way to define mapping between sets of EC2 Instance properties and firewall address groups. Address objects and an address group are created for any EC2 Instance that matches the set of specified properties, and the address group is added to the mapping's targeted address group.

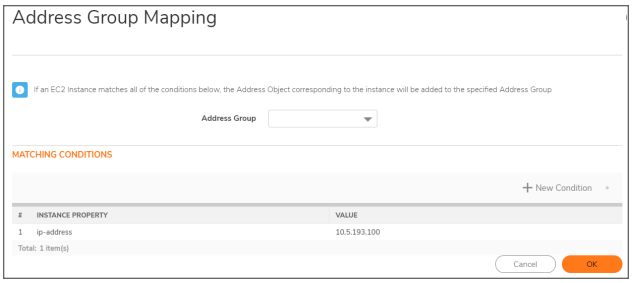
For any EC2 Instance, you can view the values of the different properties that can be used in a mapping by clicking the **Information** button in the row for the Instance. This launches a popup dialog that displays the various properties including the Instance's ID, running state, AMI, type, the VPC ID, and the different IP addresses. The user defined or custom tags, and their values, are also listed.



Creating a New Address Object Mapping

To create a new address object mapping:

1. Navigate to **OBJECT | Profile Objects > AWS**.
2. Click **New Mapping**.

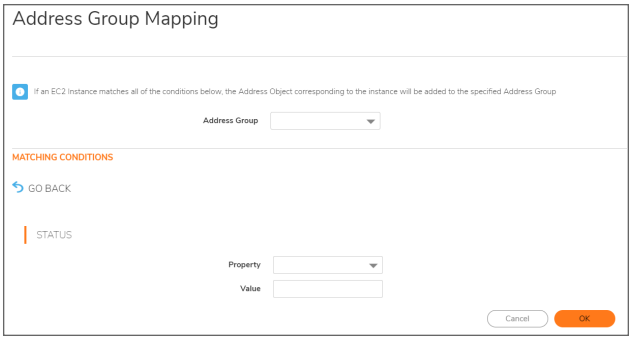


3. Select an existing **Address Group** to which you want to add the address groups representing any matched EC2 Instances.

   Only custom address groups are shown in the selection control. If you have added a custom tag to an address group, you can use this custom tag to add a new condition to the mapping.

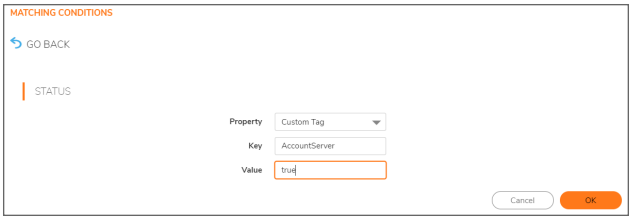
4. Click **New Condition** .

   The Mapping Condition options are displayed.



5. Select the **Property** from the drop-down menu. For example, **Custom Tag**.
6. Enter the **Key** and **Value** for the selected **Property**.

   Enter the **Value** that you want to match against, such as true.



7. Click **OK**.
8. **Go Back** to the **Address Group Mapping** dialog box.
9. Add another mapping condition if required.
   a. Click **New Condition**.
   b. Select the **Property** from the drop-down menu.
   c. Fill in the displayed fields as needed.

   d. Click **OK**.
10. **Go Back** to the **Address Group Mapping** dialog box.
11. Review the whole mapping condition you are about to create.

    Any EC2 Instance in the regions of interest that match our specified conditions (in this example, having a custom tag of *AccountsServer = true* and of type *t2.micro*) will have address objects created for each of their IP addresses. Those address objects are added to an address group, representing the EC2 Instance as a whole and that address group is added to the address group targeted in the mapping. In this example, that is the address group called *AccountsDeptServers*.
12. Edit or delete the conditions if required.

    Click the **Edit** or **Delete** icon in the **Manage** column of the condition.
13. Click **OK**.
14. Navigate to **OBJECT | Profile Objects > AWS**.
15. Click **Accept** to save the mapping.

Enable Mapping

You can create any number of address object mappings, however, they do not take effect until you enable mapping.

To enable mapping:

1. Navigate to **OBJECT | Profile Objects > AWS > Address Object Mapping**.
2. Select the **Enable Mapping**.
3. Click **Accept**.

Configuring Synchronization

The **Synchronization Interval** determines how often the firewall should check for changes and make any necessary updates to the relevant address objects and address groups.

Synchronization is needed because the address object mappings and the AWS regions being monitored can be changed or reconfigured at any time, while the IP addresses and running state of the EC2 instances may be changed on AWS.

To configure the Synchronization Interval:

1. Navigate to **OBJECT | Profile Objects > AWS > Address Object Mapping**.
2. Enter the desired number **Synchronization Interval** in seconds.
3. Click **Accept**.

To force synchronization:

1. Navigate to **OBJECT | Profile Objects > AWS**.
2. Click either **Force Synchronization** or **Delete AWS Address Objects**.
   This is useful if you are aware of changes and in a hurry to see the address objects updated accordingly.
3. Click **Accept**.
4. Click the **Refresh** so that the page reflects the latest data.

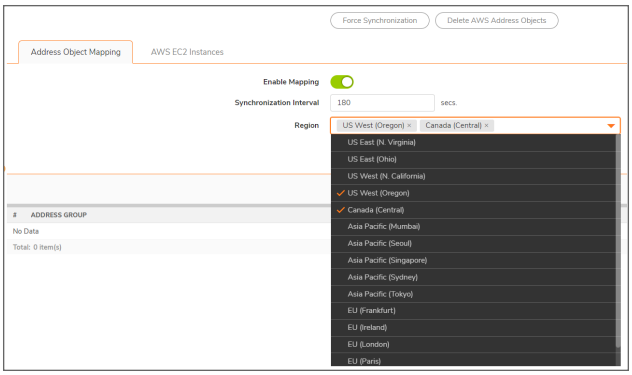
Configuring Regions to Monitor

EC2 Instances are tied to particular AWS regions. SonicOS only monitors those AWS regions of particular interest. By the default, this setting is initialized to the AWS region chosen as the Default Region during AWS configuration and used if sending firewall logs to AWS CloudWatch Logs. However, it is possible to select multiple regions to monitor and the mappings will be applied across each of those selected.

To select one or more regions to monitor:

1. Navigate to **OBJECT | Profile Objects > AWS > Address Object Mapping**.
2. Select the **Region** of interest.

   You can select the multiple regions to include in the monitor list.



3. Click **Accept**.

Verifying AWS Address Objects and Groups

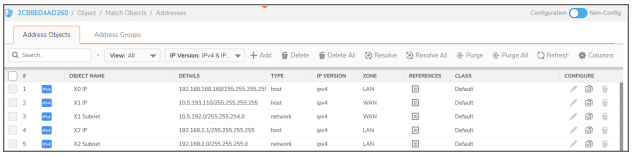
With mappings in place, a **Synchronization Interval** set, **Region** specified and, most importantly, **Mapping** enabled, you can view address objects and address groups representing the matched EC2 Instances and their IP addresses.

For example, on the AWS page itself, the address group and the mapped address groups are shown in the EC2 Instances table.

Expanding the relevant row reveals the address objects corresponding to an Instance's public and private IP addresses.

Navigating to the **OBJECT | Match Objects > Addresses** page in SonicOS and viewing the Address Object screen shows those same host address objects. VPN is used for the private IP addresses zone and WAN is used for a public address zone.

A naming convention is used for the instance address group and the address objects for each of the IP addresses, based on the Instance ID and, for the address objects, a suffix depending on whether the address is public or private.



Viewing the **Address Groups** screen and expanding the rows of interest shows that the original *AccountsDeptServers* address group now has an address group, representing an EC2 Instance, as a member.

The EC2 Instance address group itself contains the address objects that were created for each of its IP addresses.

3

ACTION PROFILES

Action Profiles feature is available only in Policy Mode .

From Action profiles, you can configure:

- Security Action Profile
- DoS Action Profile

1

Security Action Profile

Security Action Profiles define how the policies react to matching events. You can create custom Security Action Profiles or use the default Security Action Profiles.

From the **Security Action Profile** page, you can:

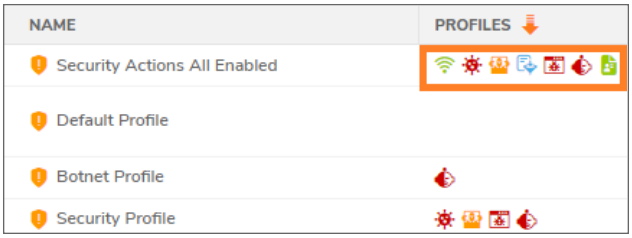
- View the Actions enabled for the Security Action Profile.
- Sort, filter, refresh, and customize the table data.
- Add, edit, clone, or delete the Security Action Profiles.

Topics:

- Security Actions
- Adding Security Action Profiles
- Editing Security Action Profiles
- Cloning Security Action Profiles
- Deleting Security Action Profiles
- Applying Security Action Profiles

Security Actions

From the **OBJECT | Action Profiles > Security Action Profile** page, you can view the actions enabled for the particular security action profile by hovering over the icons under the **PROFILES** column.



Icon	Security Action
	Bandwidth/QoS
	Anti-Virus
	Intrusion Prevention
	Anti-Spyware
	Botnet Filter
	Content Filter
	Block Page and Logging

Adding Security Action Profiles

Security Action Profiles can include any combination of profile services, with access to each service's configuration within a single page. Within the Security Action Profile page, you can configure profile options for:

- Bandwidth/QoS
- Anti-Virus
- Intrusion Prevention
- Anti-Spyware

- Botnet Filter
- Content Filter
- Block Page and Logging
- Miscellaneous

Bandwidth/QoS

From **Bandwidth/QoS**, you can configure Bandwidth and QoS Marking Profiles.

Topics:

- Bandwidth
- QoS Marking Actions
- Configuring a Bandwidth/QoS Security Action Profile

Bandwidth

Application layer BWM (bandwidth management) allows you to create a policy that regulates bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom **Security Action Profiles** configured on **OBJECT | Action Profiles > Security Action Profile** page using HTTP client, HTTP Server, Custom, and FTP file transfer types. For more information about Security Action Profiles, refer to Configuring a Bandwidth/QoS Security Action Profile.

ⓘ **IMPORTANT:** Before configuring any BWM policies, make sure to configure the Bandwidth Management profile objects on the **OBJECT | Profile Objects > Bandwidth** page according to Configuring Bandwidth Profile Objects.

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. However, with **Security Action Profiles** you can specify all content type, which you cannot do with access rules.

For a bandwidth management use case, as an administrator you might want to limit .mp3 and executable file downloads during work hours to not more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

A number of BWM action options are also available in the default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **OBJECT | Profile Objects > Bandwidth** page.

Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

QoS Marking Actions

Both 802.1p and DSCP markings are managed by SonicOS Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) provide four actions: **None**, **Preserve**, **Explicit**, and **Map**.

The default action for DSCP is **None** and the default action for 802.1p is **Preserve**.

QoS marking behavior describes the behavior of each action on both methods of marking.

QOS MARKING: BEHAVIOR

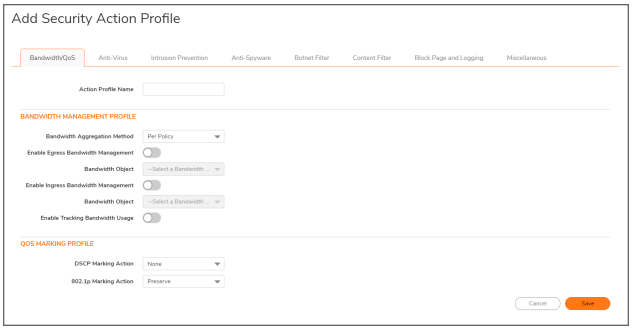
Action	802.1p (Layer 2 CoS)	DSCP (Layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) are sent out the egress interface, no 802.1p tag is added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag is explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rules (Classic Mode) or Security Action Profiles (Policy Mode) using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag is preserved.	Existing DSCP tag value is preserved.	
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that is presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that is presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.

Action	802.1p (Layer 2 CoS)	DSCP (Layer 3)	Notes
Map	The setting for QoS mapping of DSCP and 802.1p tag is defined on **OBJECT | Profile Objects > QoS Marking** page.	The setting for QoS mapping of DSCP and 802.1p tag is defined on **OBJECT | Profile Objects > QoS Marking** page. An additional check box is presented to **Allow 802.1p Marking to override DSCP values**. Selecting this check box asserts the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping only occurs in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP is mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p is mapped from the DSCP tag.

Configuring a Bandwidth/QoS Security Action Profile

To configure a Bandwidth/QoS Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. By the default, the **Add Security Action Profile** page displays the **Bandwidth/QoS** tab.



4. Select the **Bandwidth Aggregation Method** to be applied to the BWM object. For more information, refer to Bandwidth Management Methods.
   - Per Policy (default)
   - Per Action
5. Set the Bandwidth options.

Option	Description
Enable Egress Bandwidth Management	To enable BWM on outbound traffic
Enable Ingress Bandwidth Management	To enable BWM on inbound traffic

   Respective **Bandwidth Object** drop-down menu becomes active when the option is enabled.
6. Select **Bandwidth Object** from respective drop-down menu.
   - An existing BWM object
   - Create a new Bandwidth Object. For more information about creating a new bandwidth object, refer to Defining Bandwidth Profile Object Settings.
7. **Enable Tracking Bandwidth Usage** option to track bandwidth usage.

   ⓘ **NOTE:** You can enable the **Enable Tracking Bandwidth Usage** option only when the **Enable Egress Bandwidth Management** and/or **Enable Ingress Bandwidth Management** is selected.

8. Select the **QOS MARKING PROFILE** actions. For more information, refer to QoS Marking Actions.
9. Click **Save**.

Anti-Virus

SonicWall Gateway Anti-Virus (GAV) service delivers real-time virus protection directly on the SonicWall network security appliance by using SonicWall's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWall gateway. Building on SonicWall's reassembly-free architecture, SonicWall GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWall GAV delivers threat protection by matching downloaded or emailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWall's SonicAlert Team, third-party virus analysts, open source developers, and other sources.

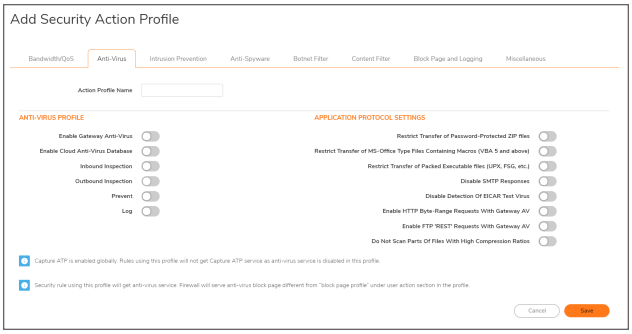
SonicWall GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols, to provide you with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWall GAV integrates advanced decompression technology that automatically decompresses and scans files on a per-packet basis.

SonicWall GAV parses supported email protocols for the header fields To, CC, and BCC. The information in these fields are displayed and logged in Capture ATP for both sender and receiver.

To configure an Anti-Virus Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.

3. Click the **Anti-Virus** tab.



4. Set the **ANTI-VIRUS PROFILE** options.

Enable Gateway Anti-Virus	To enable SonicWallGateway Anti-Virus. ⓘ **NOTE:** You must specify the zones you want SonicWall Gateway Anti-Virus protection on the **NETWORK | System > Interfaces** page.
Enable Cloud Gateway Anti-Virus Database	To enable SonicWall Anti-Virus protection if your Anti-Virus software exists in the Cloud.
Inbound Inspection	To inspect all inbound HTTP, FTP, IMAP, SMTP, and POP3 traffic. By the default, SonicWall Gateway Anti-Virus inspects all inbound HTTP, FTP, IMAP, SMTP, and POP3 traffic. Within the context of SonicWall Gateway Anti-Virus, enabling the **Inbound Inspection** protocol traffic handling refers to: • Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone. • Non-SMTP traffic from a Public zone destined to an Untrusted zone. • SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone. • SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.
Outbound Inspection	To inspect all outbound HTTP, FTP, SMTP, and TCP traffic.
Prevent	To restrict the transfer of files with specific attributes. Enabling **Prevent** restricts data file transfers for each protocol, except the TCP Stream.
Log	To keep a record of your SonicWall Gateway Anti-Virus traffic.

5. Set the **APPLICATION PROTOCOL SETTINGS** options.

Restrict Transfer of password-protected Zip files	To restrict the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.
Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)	To restrict the transfer of any MS-Office 97 and above files that contain VBA macros.
Restrict Transfer of packed executable files (UPX, FSG, etc.)	To restrict the transfer of packed executable files. Packers are utilities that compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWall Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. Additional formats are dynamically added along with SonicWall Gateway Anti-Virus signature updates.
Disable SMTP Responses	To suppress the sending of e-mail messages (SMTP) to clients from SonicWall Gateway Anti-Virus when a virus is detected in an e-mail or attachment.
Disable detection of EICAR Test Virus	To suppress the detection of the EICAR. The EICAR Standard Anti-Virus Test file is a special virus simulator file that checks and confirms the correct operation of the SonicWall Gateway Anti-Virus service.
Enable HTTP Byte-Range requests with Gateway AV	To allow the sending of byte serving, the process of sending only a portion of an HTTP message or file. The SonicWall Gateway Anti-Virus security service, by the default, suppresses the use of HTTP Byte-Range requests to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you can override the default behavior. This option is selected by the default.
Enable FTP 'REST' requests with Gateway AV	To allow the use of the FTP REST request to retrieve and reassemble sectional messages and files. The Gateway Anti-Virus service, by the default, suppresses the use of the FTP **REST** (restart) request to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.

Do not scan parts of files with high compression rates	To suppress the scanning of files, or parts of files, that have high compression rates.

6. Click **Save**.

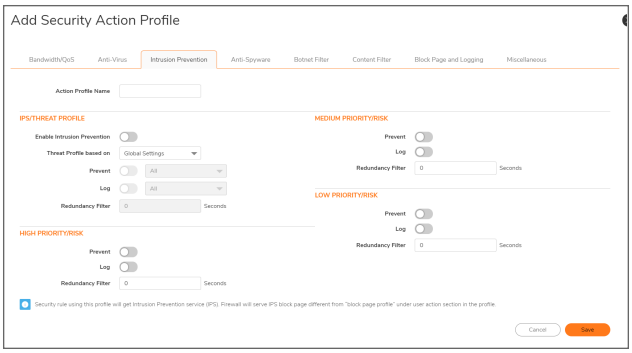
Intrusion Prevention

An Intrusion Prevention System (IPS) is a threat detection method to detect and prevent identified threats. IPS continuously monitors the network to identify the possible malicious incidents and captures information about the identified incidents. The IPS takes preventative action to prevent future attacks.

In this section, you can create Intrusion Prevention Action Profile to be used along with the Intrusion Prevention profiles created on **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles** page.

To configure a custom Intrusion Prevention Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Intrusion Prevention** tab.



4. **Enable Intrusion Prevention** to enable the SonicWall Threat Prevention Service (IPS).

5. Select the **Threat Profile** to be used to build an action profile.

Global Settings	To apply the rules defined by SonicOS. Go to step 7 if you select Global Settings.
Profile Settings	To customize the rules for a specific requirement. Skip step 7 if you select Profile Settings.

6. Select the profile to be applied to **Prevent** and **Log** from the respective drop-down menus. These options are not available if you set the **Intrusion Prevention Profile** as **Global Settings**.

Prevent	To restrict the transfer of files with specific attributes. Enabling **Prevent** restricts data file transfers for each protocol, except the TCP Stream.
Log	To keep a record of your SonicWallIntrusion Prevention traffic.

You can select the default or custom **Profiles** created on **OBJECT | Profile Objects > Intrusion Prevention > Intrusion Prevention Profiles** page. For more information, refer to Adding Intrusion Prevention Profiles.

7. Set the **Redundancy Filter** value in seconds for how long to use these filters.
8. Select the **Low**, **Medium**, and **High** Priority/Risk options based on your needs to **Prevent**, **Log**, and for how long to use the **Redundancy Filters**.

   ⓘ **NOTE:** Low, Medium, and High Priority/Risk options are not available if you select **Profile Settings** because your Intrusion Prevention Profile addresses those capabilities.

9. Click **Save**.

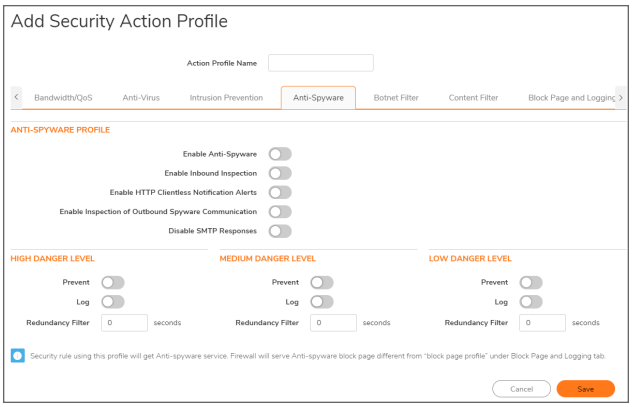
Anti-Spyware

An Anti-Spyware is a spyware protection, designed to detect, prevent, and remove spyware and adware infections. An Anti-Spyware actively scans inbound and outbound traffic from e-mails, websites, and downloaded files to block spyware from entering the system. The detection works based on rules.

In this section, you can create Anti-Spyware Security Action Profile objects.

To configure an Anti-Spyware Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Anti-Spyware** tab.



4. Set the **ANTI-SPYWARE PROFILE** options:

Enable Anti-Spyware	To activate SonicWall's Anti-Spyware protection.
Enable Inbound Inspection	To make inbound traffic available for inspection.
Enable HTTP Clientless Notification Alerts	To show an error message when a request is blocked.
Enable Inspection of Outbound Spyware Communication	To make outbound traffic available for inspection.
Disable SMTP Responses	To suppress the sending of e-mail messages (SMTP) to clients from SonicWall Anti-Spyware when a virus is detected in an e-mail or attachment.

5. Select the profile to be applied to **Prevent** and **Log** from the respective drop-down menu.

Prevent	To restrict the transfer of files with specific attributes. Enabling **Prevent** restricts data file transfers for each protocol, except the TCP Stream.
Log	To keep a record of your SonicWallAnti-Spyware traffic.

6. Set the **Redundancy Filter** value in seconds for how long to use these filters.
7. Select the **Low**, **Medium**, and **High** Danger Level options based on your needs to **Prevent**, **Log**, and for how long to use the **Redundancy Filters**.

   ⓘ **NOTE:** Low, Medium, and High Danger Level options are not available if you select **Profile Settings** because your Anti-Spyware Profile addresses those capabilities.

8. Click **Save**.

Botnet Filter

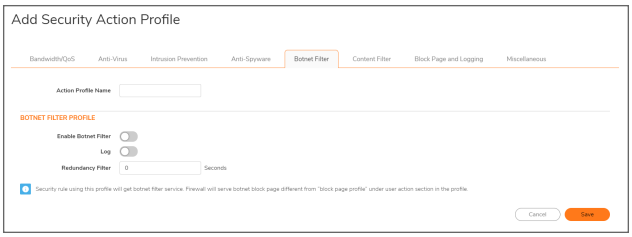
Botnet is the collection of devices connected to internet like computers, mobile phones, IoT devices, Smart Television, and others that are compromised with malware programs. It is becoming popular among cyber criminals due to its ability to infiltrate any device that is connected to the internet.

Using botnets, cyber criminals can execute DDoS attacks and generate a network of fraud advertisement through E-mail Spamming.

In this section, you can create a Botnet Filtering Security Action Profile to prevent malware programs from entering the connected devices.

To configure a Botnet Filter Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Botnet Filter** tab.



4. Select **Enable Botnet Filter** to activate SonicWall's Botnet Filtering service.
5. Select the **Log** to record the list of malware programs blocked.
6. Enter the **Redundancy Filters** value in seconds for how long to use the profile.
7. Click **Save**.

Content Filter

SonicWall Content Filtering service compares the requested web sites against a massive database in the cloud containing millions of rated URLs, IP addresses, and web sites.

From Content Filtering, you can create Content Filtering Service (CFS) Security Action Profile that allow or deny access to sites based on individual or group identity.

To configure a Content Filter Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
   - None
   - Confirm
   - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Configure the content filter profiles.
   - General
   - Passphrase
   - Confirm
   - Consent
   - Custom Header

   Blocked pages served are different from the General action profile section of this profile.
7. Click **Save**.

General

General action profile helps to enable the options listed below:

- HTTPS content filtering solution to inspect the contents of secure websites in addition to regular websites.
- Safe Search to filter explicit content from search results.
  You can lock Safe Search if you want to keep Safe Search turned on and prevent users from turning it off.
- Wipe cookies.

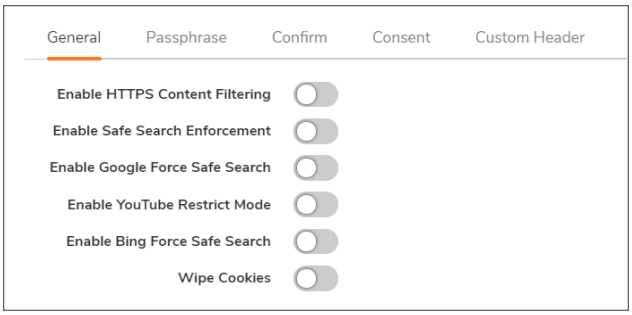
To configure General action profile of the Content Filter:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:

- Add a new Security Action Profile.
    1. Click the **Add** icon.
    2. Enter an **Action Profile Name**.
- Edit an existing Security Action Profile.
  Hover over an existing Security Action Profile and click the **Edit** icon.

3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
    - None
    - Confirm
    - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Scroll to the **General** option.



7. Set the **General** action profile options.

Enable HTTPS Content Filtering	To enable content filtering for HTTPS sites. HTTPS content filtering is IP based and does not inspect the URL, but uses other methods to obtain the URL rating. When this option is enabled, CFS performs URL rating lookup in this order: • Searches the client hello for the *Server Name*, which CFS uses to obtain the URL rating. • If the Server Name is not available, searches the SSL certificate for the *Common Name*, which CFS uses to obtain the URL rating. • If neither Server Name nor Common Name is available, CFS uses the *IP address* to obtain the URL rating. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages are silently blocked.

Enable Safe Search Enforcement	To enforce Safe Search when searching on any of the following websites: • www.yahoo.com • www.ask.com • www.dogpile.com • www.lycos.com This enforcement cannot be configured at the policy level as the function employs DNS redirection to HTTPS sites. For HTTPS sites, client DPI-SSL with content filter must be enabled.
Enable Google Force Safe Search	To override the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action. Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.
Enable YouTube Restrict Mode	To access YouTube in Restrict (Safe Search) mode. YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. When this feature is enabled, SonicOS rewrites the DNS response for the YouTube domain to its Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.
Enable Bing Force Safe Search	To override the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action. When this feature is enabled, SonicOS rewrites the DNS response for the Bing domain to its Safe Search virtual IP address. This feature takes effect only after the DNS cache of the client host is refreshed.
Wipe Cookies	To remove cookie trace pages of visited websites.

8. Click **Save**.

Passphrase

Passphrase helps to build a password-protected web page. Only authorized users can access the password-protected web page by entering the correct password which was set during the page build.

To create a password-protected web page:

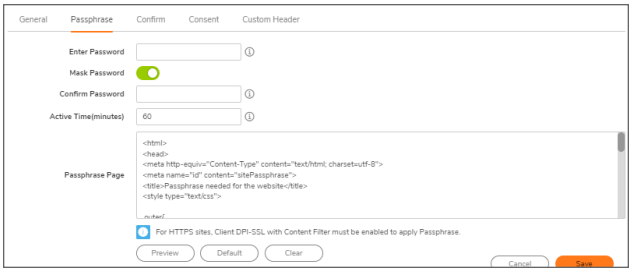
1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
    - Add a new Security Action Profile.
        1. Click the **Add** icon.
        2. Enter an **Action Profile Name**.

- Edit an existing Security Action Profile.

  Hover over an existing Security Action Profile and click the **Edit** icon.

3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
   - None
   - Confirm
   - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Scroll to the **Passphrase** option.

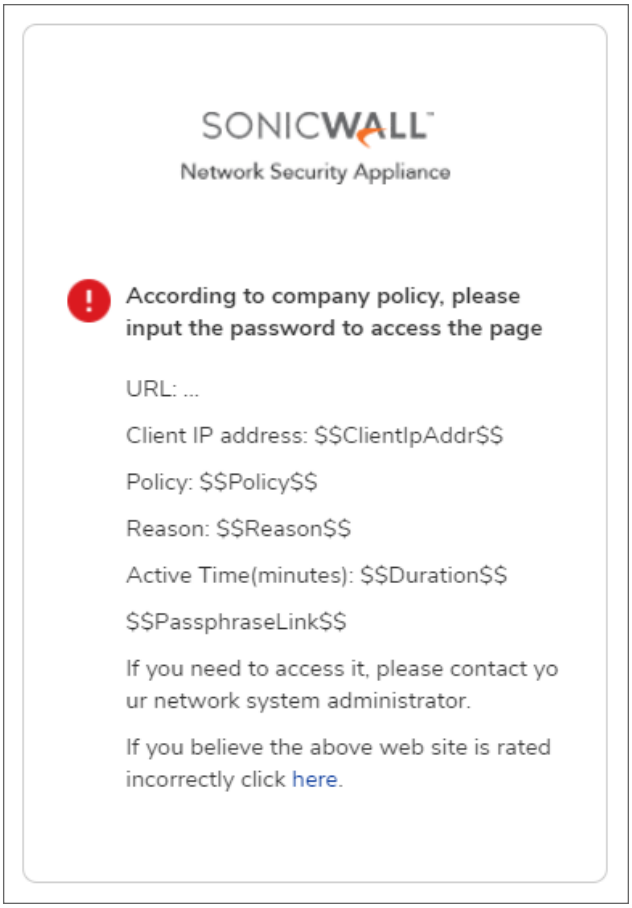


7. Enter the passphrase or password for the website in the **Enter Password** field. The password can be up to 64 characters.

   ⓘ **NOTE:** The **Mask Password** option is enabled by the default. Disabling this option converts the password into plain text and the entry in the **Confirm Password** field becomes visible.
8. Enter the same passphrase or password again in the **Confirm Password** field.
9. Enter the effective duration, in minutes, for a passphrase based on category or domain in the **Active Time (minutes)** field.

   The minimum time is 1, the maximum is 9999, and the default is **60**.
10. Do one of the following with **Passphrase Page** code:
    a. No action is required to continue with the default web page.
    b. Make the necessary changes to the default code if you want to customize the web page.
    c. Click **Clear** to enter your own code for a new web page.

11. Click **Preview** to preview the web page.



If you continue with the default web page, website URL, Client IP address, policy, reason, and active minutes along with a field for entering the password are shown in the preview.

12. Click **Close** to go back to Security Action Profile page.
13. Click **Default** if you wish to continue with the default blocked page.
14. Click **Save**.

Confirm

Confirm helps to build a restricted web page that requires the user confirmation to access.

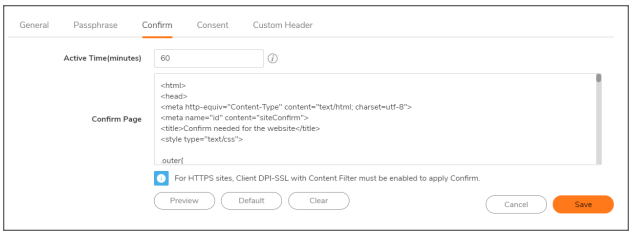
ⓘ **NOTE:**

- Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page.
- For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Confirm. For more information, refer to About Confirm Feature.

To create a restricted web page that requires confirmation:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
   - None
   - Confirm
   - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Scroll to the **Confirm** option.



7. Enter the effective duration, in minutes, for a confirmed user based on category or domain in the **Active Time (minutes)** field.
   The minimum time is 1, the maximum is 9999, and the default is **60**.
8. Do one of the following with **Confirm Page** code:

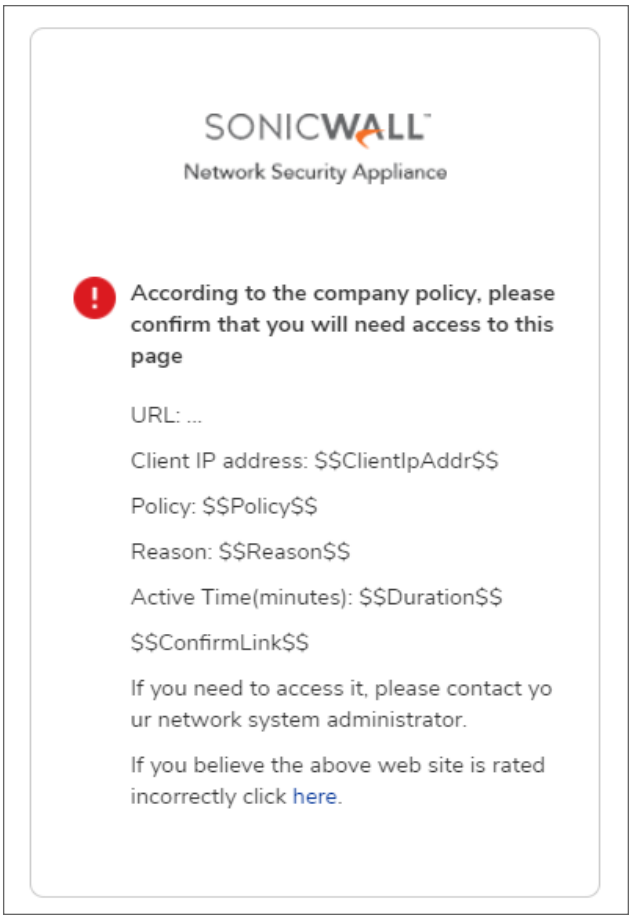
a. No action is required to continue with the default web page.

b. Make the necessary changes to the default code if you want to customize the web page.

c. Click **Clear** and enter your own code for a new web page.

9. Click **Preview** to preview the web page.

   If you continue with the default web page, web site URL, Client IP address, policy, reason for the block, and active minutes along with a field for entering the confirmation are shown in the preview.



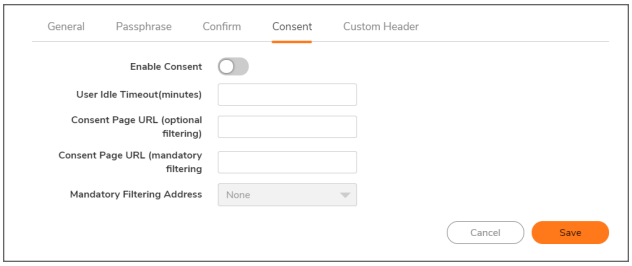
10. Click **Close** to go back to Security Action Profile page.

11. Click **Default** if you wish to continue with the default blocked page.

12. Click **Save**.

Consent

NOTE: Consent only works for HTTP requests. HTTPS requests cannot be redirected to a **Confirm** (consent) page.



To create a web page that requires consent:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
   - None
   - Confirm
   - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Scroll to **Consent** option.
7. **Enable Consent** to display the Consent (Confirm) page when a user visits a site requiring consent before access.
   When this option is selected, the other options become available.

8. Set the **Consent** page options:

User Idle Timeout (minutes)	To remind users about the remaining time left to expire by displaying the **Consent** page. The minimum idle time is one minute, the maximum is 9999 minutes, and the default is 15 minutes.

Consent Page URL (optional filtering)	To enter URL of the website where a user is redirected if they go to a website requiring consent.
	The **Consent** page must:
	• Reside on a web server and be accessible as a URI by users on the network.
	• Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
	  • Unfiltered access: `<appliance's LAN IP address>/iAccept.html`
	  • Filtered access: `<appliance's LAN IP address>/iAcceptFilter.html`

Consent Page URL (mandatory filtering	To enter URL of the website where the user is redirected if they go to a website requiring mandatory filtering. The **Consent** page must: • Reside on a web server and be accessible as a URI by users on the network. • Contain a link to the `<appliance's LAN IP address>/iAcceptFilter.html` page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.
Mandatory Filtering Address	To select an Address Object that contains the configured IP addresses requiring mandatory filtering. You can select the default or custom address objects created on the **OBJECT | Match Objects > Addresses > Address Objects** page. For more information, refer to Adding Address Objects. ⓘ | **NOTE:** Make sure that **Enable Consent** is enabled to activate this feature.

9. Click **Save**.

Custom Header

From SonicOS 6.5.1 and later, you can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

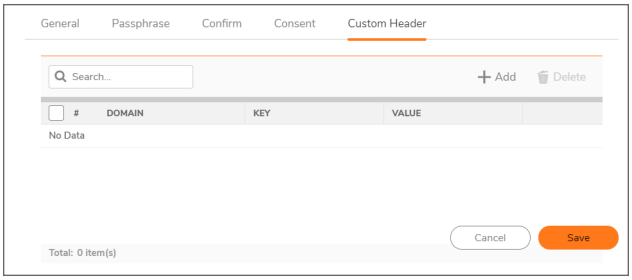
ⓘ | **IMPORTANT:** Before configuring the Custom Header, make sure that:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.

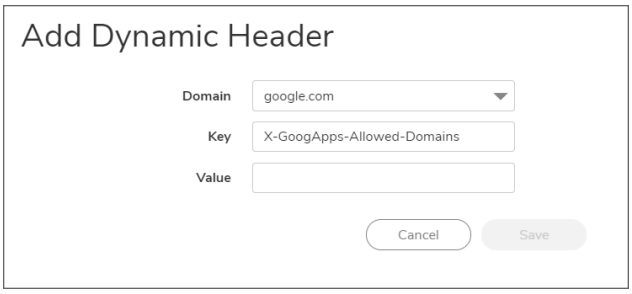
To configure a CFS custom header and enable custom header insertion:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Content Filter** tab.
4. **Enable Content Filtering** to activate SonicWall's Content Filtering service.
5. Select a **Content Filter Action**.
   - None
   - Confirm
   - Passphrase

   The content filter action is applied to your security rule using the profile that has the action set to CFS.
6. Scroll to the **Custom Header** tab.



7. Click the **Add** icon to configure the **Domain**, **Key**, and **Value** for the custom Dynamic Header entry.



8. Click **Save**.
   The Header appears in the Custom Header list.
9. Click **Save**.

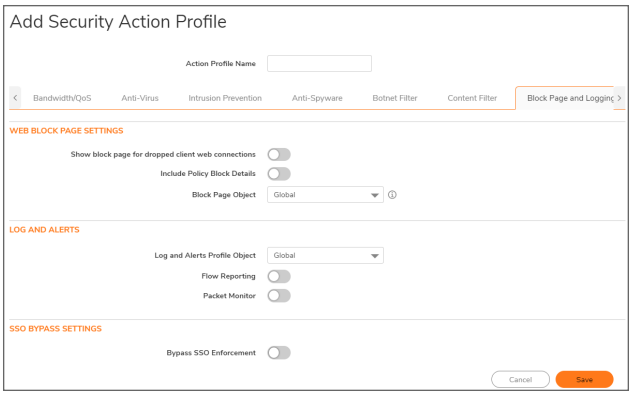
Block Page and Logging

In this section, you can use:

- The default Block Page profile or create a custom Block Page profile on **OBJECT | Profile Objects > Block Page**. For more information, refer to Adding Custom Block Pages.
- The default Log and Alerts profile or create a custom Log and Alerts profile on **OBJECT | Profile Objects > Log and Alerts**. For more information, refer to Adding Log and Alerts Profiles.

To configure the Block Page and Logging Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.
3. Click the **Block Page and Logging** tab.



4. Set the **Web Block Page Settings** options:

Show block page for dropped client web connections	To show the Global, Default, or custom Block Page you created in Profiles for dropped client web connections.
Include Blocking Policy Details	To include the reason for the dropped connections.

Block Page Object	Select the **Block Page Object** from the drop-down menu. You can use the **Global** page, a **Default Block Page**, or a custom Block Page that you created on **OBJECT | Profile Objects > Block Page**. For more information, refer to Adding Custom Block Pages.

5. Set **LOG AND ALERTS** options:
   a. Select the **Log and Alerts Profile Object**.
      You can use the **Default** or a custom log and alerts profile that you created on **OBJECT | Profile Objects > Log and Alerts**. For more information, refer to Adding Log and Alerts Profiles.
   b. Enable **Flow Reporting**.
   c. Enable **Packet Monitor** to capture the packets that match the Security Policy.
6. Set **SSO Bypass Settings** options:
   a. Enable **Bypass SSO Enforcement**.
7. Click **Save**.

Miscellaneous

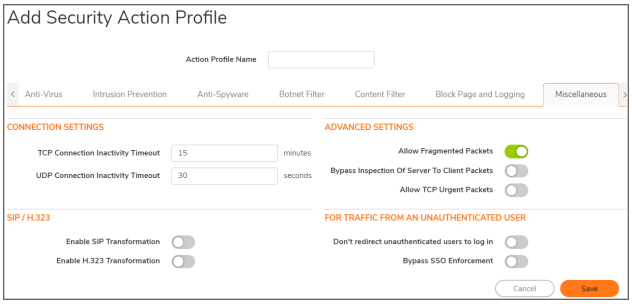
From **Miscellaneous** section, you can define additional settings in relation to your profiles and action objects.

- The connection inactivity timeout of the web page
- The protocol to be used for data transfer
- Access to unauthenticated users
- Settings with respect to packets

To add or modify Miscellaneous settings:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
   - Add a new Security Action Profile.
     1. Click the **Add** icon.
     2. Enter an **Action Profile Name**.
   - Edit an existing Security Action Profile.
     Hover over an existing Security Action Profile and click the **Edit** icon.

3. Click the **Miscellaneous** tab.



4. Modify **Connection Settings**, **Advanced Settings**, **SIP/H.323 Transformation settings**, and so on.
5. Set the **Miscellaneous** settings.

Setting	Option	Description
CONNECTION SETTINGS	TCP Connection Inactivity Timeout	Set inactivity timeout in minutes to terminate the TCP connection. The default value is 15 minutes.
	UDP Connection Inactivity Timeout	Set inactivity timeout in seconds to terminate the UDP connection. The default value is 30 seconds.
ADVANCED SETTINGS	Allow Fragmented Packets	Enable this option to allow fragmented packets (traffic) to pass across VPN tunnels successfully. This option is enabled by the default.
	Bypass Inspection Of Server To Client Packets	Enable this option to bypass inspection of server to client packets. This option is disabled by the default.
	Allow TCP Urgent Packets	Enable this option to allow TCP urgent packets. This option is disabled by the default.
SIP / H.323	Enable SIP Transformation	Enable this option to transform SIP messages between LAN (trusted) and WAN/DMZ (untrusted). **NOTE:** SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa. This option is disabled by the default.
	Enable H.323 Transformation	Enable this option to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWall security appliance. This option is disabled by the default.

Setting	Option	Description
FOR TRAFFIC FROM AN UNAUTHENTICATED USER	Don't redirect unauthenticated users to log in	Enable this option to stop redirecting unauthenticated users to log in. This option is disabled by the default.
	Bypass SSO Enforcement	Enable this option to bypass the SSO authentication of the devices. This option is disabled by the default.

6. Click **Save**.

Editing Security Action Profiles

To edit a Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Hover over the security action profile to be edited and click the **Edit** icon.
3. Make the necessary changes. For more information, refer to Adding Security Action Profiles.
4. Click **Save**.

Cloning Security Action Profiles

ⓘ | **NOTE:** You can clone from the default profiles also.

To clone from an existing Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Hover over the security action profile you want to clone and click the **Clone** icon.
   This creates a duplicate of the page, which allows you to create a new security action profile based on your requirement.
3. Make the necessary changes.
   For more information, refer to Adding Security Action Profiles.
4. Click **Save**.

Deleting Security Action Profiles

ⓘ **NOTE:** Only custom Security Action Profiles can be deleted. You cannot delete the Default Security Action Profiles.

To delete a custom Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Hover over the Security Rule Action Object to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom Security Action Profiles:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Do one of the following:
    a. Select check boxes of the security action profile to be deleted.
    b. Select the check box in the table header to select all custom security action profiles.
3. Click the **Delete** icon on top of the table.
4. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.

Applying Security Action Profiles

Once the Security Action Profiles are created, you can apply them in configuring security policies on **POLICY | Rules and Policies > Security Policy** page.

For more information, refer to **Security Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

2

DoS Action Profile

DoS Action Profiles are action profiles that can be established to protect DoS related activity such as:

- Flood Protection
- DDoS Protection
- Attack Protection
- Connection Limiting

From the DoS Action Profile page, you can:

- View the Actions enabled for the DoS Action Profile.
- Sort, filter, refresh, and customize the table data.
- Add, edit, clone, or delete the DoS Action Profiles.

Topics:

- DoS Actions
- Adding DoS Action Profiles
- Editing DoS Action Profiles
- Cloning DoS Action Profiles
- Deleting DoS Action Profiles
- Applying DoS Action Profiles

DoS Actions

From the **OBJECT | Action Profiles > DoS Action Profile** page, you can view the actions enabled for the particular DoS action profile by hovering over the icons under the **PROFILES** column.

Icon	DoS Action
	SYN Flood Protection
	UDP Flood Protection
	ICMP Flood Protection
	DDoS Protection
	Attack Protection
	Connection Limiting

Adding DoS Action Profiles

SonicOS monitors UDP or ICMP traffic flow to defined destinations to defend against UDP or ICMP flood attacks. UDP or ICMP packets to a specified destination are dropped if one or more sources exceeds the configured threshold.

Topics:

- Flood Protection
- DDoS Protection
- Attack Protection
- Connection Limiting

Flood Protection

The Flood Protection allows you to:

- Manage:
  - TCP (Transmission Control Protocol) traffic settings such as Layer 2 SYN/RST/FIN Flood Protection or Layer 3 SYN Flood Protection - SYN Proxy, WAN DDoS Protection
  - UDP Flood Protection
  - ICMP Flood Protection or ICMPv6 flood protection
- View statistics through the security appliance:
  - TCP traffic
  - UDP traffic
  - ICMP or ICMPv6 traffic

To configure the Flood Protection:

From the Flood Protection, you can configure the below listed protections:

- Layer 3 SYN Flood Protection - SYN Proxy
- Layer 2 SYN/RST/FIN Flood Protection
- UDP Flood Protection
- ICMP Flood Protection

Layer 3 SYN Flood Protection - SYN Proxy

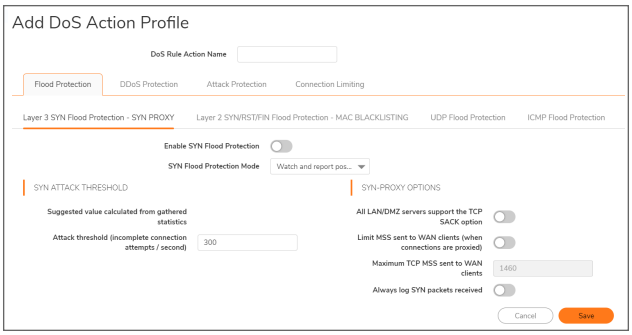
A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection.

To configure the Layer 3 SYN Flood Protection - SYN Proxy:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.

     Hover over an existing DoS Action Profile and click the **Edit** icon.

   By the default, the **Add DoS Action Profile** page opens with the **Flood Protection > Layer 3 SYN Flood Protection - SYN Proxy** option.



3. **Enable Syn Flood Protection** to enable a SYN Flood Protection mode.
4. Select the protection mode from the **SYN Flood Protection Mode** drop-down menu.

Watch and Report Possible SYN Floods	To monitor SYN traffic on all interfaces and logs suspected SYN flood activity that exceeds a packet-count threshold. This option does not actually turn on the SYN Proxy on the device, so the device forwards the TCP three-way handshake without modification. **NOTE:** • This is the least invasive level of SYN flood protection. • Select this option if your network is not in a high-risk environment. • When this protection mode is selected, the **SYN-Proxy** options do not apply.
Proxy WAN Client Connections When Attack is Suspected	To enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second exceeds a specified threshold. This method ensures that the device continuous to process valid traffic during the attack, and make sure that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. **NOTE:** • This is the intermediate level of SYN Flood protection. • Select this option if your network sometimes experiences SYN Flood attacks from internal or external sources.
Always Proxy WAN Client Connections	To set the device to always use SYN Proxy. **NOTE:** • This method blocks all spoofed SYN packets from passing through the device. This is an extreme security measure, which directs the device to respond to port scans on all TCP ports. The SYN Proxy feature forces the device to respond to all TCP SYN connection attempts, which can degrade performance and generate false positive results. • Select this option only if your network is in a high-risk environment.

5. Modify the **Attack threshold (incomplete connection attempts / second)** value if required.
6. Set the **SYN-PROXY OPTIONS**.

For **SYN Proxy Options**, if one of the higher levels of SYN Protection is selected, SYN-Proxy options can be selected to provide more control over what is sent to WAN clients when in SYN Proxy mode. When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server responds to the TCP options normally provided on SYN/ACK packets.

All LAN/DMZ servers support the TCP SACK	To enable SACK (Selective Acknowledgment), so that when a packet is dropped, the receiving device indicates which packets it received. Enable this option only when all servers covered by the firewall that are accessed from the WAN support the SACK option.
Limit MSS sent to WAN clients (when connections are proxied	To enable **Maximum TCP MSS sent to WAN clients** option.
Maximum TCP MSS sent to WAN clients	To enter the maximum MSS (Minimum Segment Size) value. The default is 1460, the minimum value is 32, and the maximum is 1460. This sets the threshold for the size of TCP segments, preventing a segment that is too large from being sent to the targeted server. For example, if the server is an IPsec gateway, it might need to limit the MSS it receives to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment makes it possible to control the manufactured MSS value sent to WAN clients. If you specify an override value for the default of 1460, only a segment of the same size or smaller is sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.
Always log SYN packets received	To log all SYN packets received. This option is only available with higher levels of SYN protection. When using Proxy WAN client connections, remember to set these options conservatively as they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can continue during an attack.

7. Click **Save**.
8. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

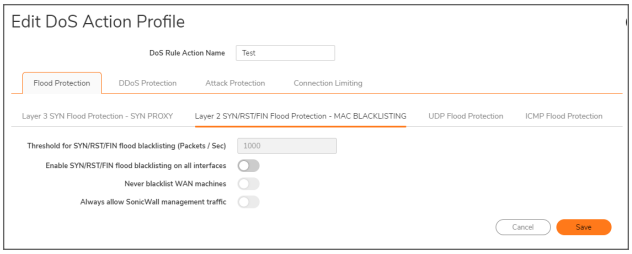
Layer 2 SYN/RST/FIN Flood Protection

The SYN/RST/FIN Blacklisting feature lists devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

To configure the Layer 2 SYN/RST/FIN Flood Protection:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.
3. Click **Flood Protection > Layer 2 SYN/RST/FIN Flood Protection** option.



4. **Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces** to enable the blacklisting feature on all interfaces on the firewall and change the default settings.
5. Make the necessary changes to the default settings.

Never blacklist WAN machines	To always skip adding WAN systems to the SYN Blacklist. This option is recommended as leaving it cleared may interrupt traffic to and from the firewall's WAN ports.
Always allow SonicWall management traffic	To skip filtering of the IP traffic from a blacklisted device targeting the firewall's WAN IP addresses. This allows management traffic and routing protocols to maintain connectivity through a blacklisted device.

Threshold for SYN/RST/FIN flood blacklisting	To specify the maximum number of SYN, RST, FIN, and TCP packets allowed per second. The minimum is 10, the maximum is 800000, and the default is 1000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

6. Click **Save**.
7. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

UDP Flood Protection

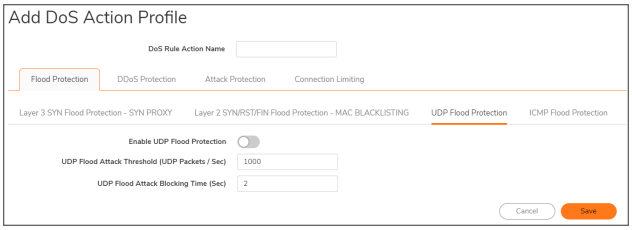
UDP Flood Attacks are a type of denial-of-service (DoS) attack. They are initiated by sending a large number of UDP packets to random ports on a remote host. As a result, resources of the victimized system are consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients.

SonicWall UDP Flood Protection defends against these attacks by using a *watch and block* method. The appliance monitors UDP traffic to a specified destination. If the rate of UDP packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent UDP packets to protect against a flood attack.

UDP packets that are DNS query or responses to or from a DNS server configured by the appliance are allowed to pass, regardless of the state of UDP Flood Protection.

To configure UDP Flood Protection:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.
3. Click **Flood Protection > UDP Flood Protection** option.



4. **Enable UDP Flood Protection** to enable UDP flood protection and enable the other UDP Flood Protection options.
5. Make the necessary changes to the default values.

UDP Flood Attack Threshold	The maximum number of UDP packets allowed per second to be sent to a host, range, or subnet that triggers UDP Flood Protection. Exceeding this threshold triggers UDP Flood Protection. The minimum value is 50, the maximum value is 1000000, and the default value is 1000.
UDP Flood Attack Blocking Time	After the appliance detects the rate of UDP packets exceeding the attack threshold for this duration of time, UDP Flood Protection is activated and the appliance begins dropping subsequent UDP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.

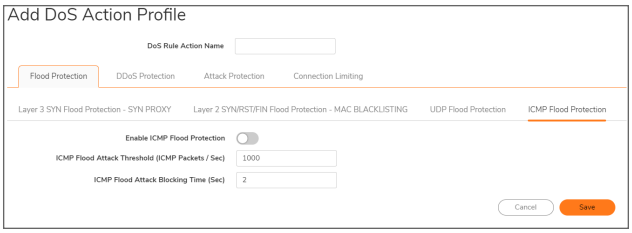
6. Click **Save**.
7. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

ICMP Flood Protection

ICMP Flood Protection functions similar to UDP Flood Protection, except it monitors for ICMPv4/ICMPv6 Flood Attacks. The only difference is that DNS queries are not allowed to bypass ICMP Flood Protection.

To configure ICMP Flood Protection:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.
3. Click **Flood Protection > ICMP Flood Protection** option.



4. **Enable ICMP Flood Protection** to enable ICMP flood protection and enable the other ICMP Flood Protection options.
5. Make the necessary changes to the default values.

ICMP Flood Attack Threshold	The maximum number of ICMP packets allowed per second to be sent to a host, range, or subnet. The minimum number is 10, the maximum number is 100000, and the default number is 1000.
ICMP Flood Attack Blocking Time	After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood Protection is activated, and the appliance begins dropping subsequent ICMP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.

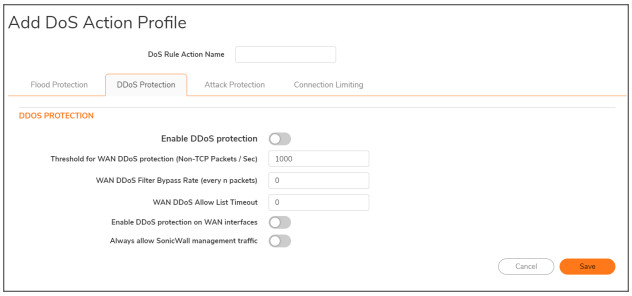
6. Click **Save**.
7. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

DDoS Protection

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target.

To configure the DDoS Protection of the DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.
3. Click the **DDoS Protection** tab.



4. Click **Enable DDoS protection**.
5. Make the necessary changes to the **DDoS Protection** default settings.

Threshold for WAN DDoS protection (Non-TCP packets / Sec)	To set the threshold value of non-TCP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers WAN DDoS flood protection. The minimum number is 0, the maximum number is 10000000, and the default number is 1000. ⓘ | **NOTE:** This option is applicable when **Enable DDOS protection** is selected.
WAN DDoS Filter Bypass Rate (every n packets)	To set the WAN DDoS filter bypass rate. The default value of the WAN DDoS Filter Bypass Rate is 0. This default rate prevents all packets passing through, unless the device from which they originate is on the Allow List. This can be an appropriate choice in some deployments. When you configure this rate to a non-zero number, some non-TCP packets that would normally be dropped by WAN DDoS Protection are passed to the LAN/DMZ network. A non-zero bypass rate allows the risk of a potential attack to be reduced, but not completely blocked. Allowing some packets to pass through (such as every 3rd packet), even though their sources are not on the Allow List, can provide a mechanism by which legitimate WAN-side hosts can get a packet through to the LAN/DMZ side, in spite of the high alert status of the appliance. You must determine the appropriate value to set, depending on the capabilities of the potential LAN-side target machines and the nature of the legitimate non-TCP traffic patterns in the network. ⓘ | **NOTE:** This option is applicable when **Enable DDOS protection** is selected.
WAN DDoS Allow List Timeout - seconds	To set expire timeout for devices added in the allow list. If a non-zero Allow List Timeout is defined by the user, entries in the Allow List expire in the configured time. If the Allow List Timeout is zero, they never expire. In either case, the least-recently-used entry in a particular group can be replaced by a new entry, if no unused entry is available in the list.

Enable WAN DDoS Protection on WAN interfaces	To provide protection against non-TCP DDoS attacks. Use this option in combination with SYN-Flood Protection if TCP SYN-flood attacks are a concern. This option is not intended to protect a well-known server of non-TCP services on the Internet (such as a central DNS server), but is intended to protect LAN and DMZ networks for which the majority of non-TCP traffic is initiated from the LAN/DMZ side, possibly in combination with limited WAN-initiated traffic. When WAN DDoS Protection is enabled, it tracks the rate of non-TCP packets arriving on WAN interfaces. When the rate of non-TCP packets exceeds the specified threshold, non-TCP packets arriving on WAN interfaces will be filtered. A non-TCP packet is only forwarded when at least one of the following conditions is met: • The source IP address is on the Allow list • The packet is SonicWall management traffic and **Always allow SonicWall management traffic** is selected • The packet is an ESP packet and matches the SPI of a tunnel terminating on the network security appliance • The packet is the nth packet matching the value specified for **WAN DDoS Filter Bypass Rate (every n packets)** If none of the above conditions are met, the packet is dropped early in packet processing.
Always allow SonicWall management traffic	To allow the traffic that is needed to manage your SonicWall appliances to pass through your WAN gateways, even when the appliance is under a non-TCP DDoS attack.

6. Click **Save**.
7. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

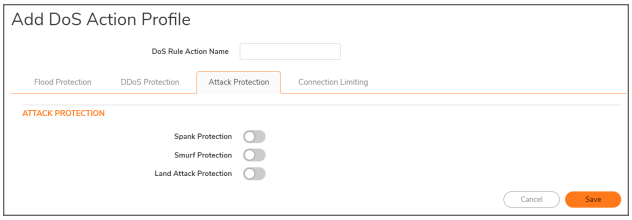
Attack Protection

From the **Attack Protection**, you can guard the network against remote host attacks, smurf attacks, and a Layer 4 Denial of Service (DoS) attacks.

To configure the Attack Protection of the DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.

3. Click the **Attack Protection** tab.



4. Enable the **Attack Protection** options.

Spank Protection	To guard against remote host attacks responding to TCP packets that have come from a multicast IP addresses. Attackers exploit this vulnerability by conducting a *spank* denial of service attack. This results in the host being shut down or the network traffic reaching saturation. Also, this vulnerability can be used by an attacker to conduct stealth port scans against the host.
Smurf Protection	To guard against attacks where LAN Clients are being used as part of an *Amplifier network*.
Land Attack Protection	To protect against a Layer 4 Denial of Service (DoS) attack where the attacker resets the source and destination information of a TCP segment to be the same. A vulnerable machine crashes or freezes because the packet is being repeatedly processed by the TCP stack.

5. Click **Save**.
6. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

Connection Limiting

The **Connection Limiting** feature is intended to offer an additional layer of security and control when coupled with features such as SYN Cookies and Intrusion Prevention Services (IPS). Connection Limiting provides a means of throttling connections through the firewall using Security Policies as a classifier and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted > Untrusted traffic (that is, LAN > WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection Limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, Connection Limiting can be used to protect publicly available servers (such as, web servers) by limiting the number of legitimate inbound connections permitted to the server (that is, to protect the server against the Slashdot-effect). This is different from SYN flood protection that attempts to detect and prevent partially-open or spoofed TCP connection. This is most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

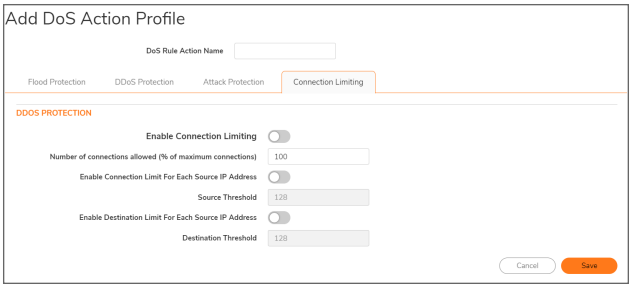
Connection Limiting is applied by defining a percentage of the total maximum allowable connections that might be allocated to a particular type of traffic.

More specific rules can be constructed. For example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

It is not possible to use IPS signatures as a Connection Limiting classifier; only Security Policies (for example, Address Objects and Service Objects) are permissible.

To configure the Connection Limiting of the DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Add a new DoS Action Profile.
     1. Click the **Add** icon.
     2. Enter a friendly **DoS Rule Action Name**.
   - Edit an existing DoS Action Profile.
     Hover over an existing DoS Action Profile and click the **Edit** icon.
3. Click the **Connection Limiting** tab.



4. **Enable Connection Limiting**.
5. Configure options and thresholds as necessary.
6. Click **Save**.
7. Click **Cancel** to go back to the **DoS Action Profile** page or proceed with other configurations.

Editing DoS Action Profiles

ⓘ | **NOTE:** You cannot edit the default profiles.

To edit a DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Hover over the **DoS Action Profile** to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding DoS Action Profiles.
4. Click **Save**.

Cloning DoS Action Profiles

ⓘ | **NOTE:** You can clone from the default profiles also.

To clone from an existing DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Hove over the DoS Action Profile to be cloned and click the **Clone** icon.
   This creates a duplicate of the page, which allows you to create a new DoS Action Profile using the similar content.
3. Make the necessary changes to the **Clone DoS Action Profile** form.
   For more information, refer to Adding DoS Action Profiles.
4. Click **Save**.

Deleting DoS Action Profiles

NOTE:

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete a custom DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Hover over the DoS Action Profile to be deleted from the list and click the **Delete** icon.
3. Click **OK** in the confirmation dialog box.

To delete multiple or all custom DoS Action Profiles:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Do one of the following:
   - Select check boxes of the items to be deleted and click the **Delete** icon on top of the table.
   - Select the check box in the table header and click the **Delete** icon on top of the table.
     All custom items get selected.
3. Click **Incremental Delete** to delete the selected items one-by-one and view individual item status.

Applying DoS Action Profiles

Once the DoS Action Profiles are created, you can apply them in configuring Security policies and DoS policies on **POLICY | Rules and Policies** page. For more information, refer to SonicOS 7.0 Rules and Policies Administration Guide for Policy Mode.

4

ACTION OBJECTS

Action Objects feature is available only in Classic Mode.

From Action Objects, you can configure:

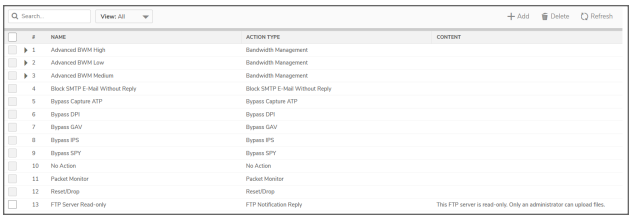
- App Rule Actions
- Content Filter Actions

1

App Rule Actions

From the **App Rule Actions** page, you can define reactions when the **App Rule** policy matches the events and gives the list of default and custom action objects. From this page, you can:

- Filter the table data
- Refresh and sort the table data to identify the specific results
- Create, edit, and delete custom action objects for the listed Actions



Topics:

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can create a custom action object or select one of the default action objects.

Topics:

- Default Action Objects
- Action Types for Custom Action Objects

Default Action Objects

SonicOS comes with the number of default action objects. These default action objects cannot be edited or deleted.

You can select a default action object while adding or editing an app control policy on the **POLICY | Rules and Policies > App Rules** page.

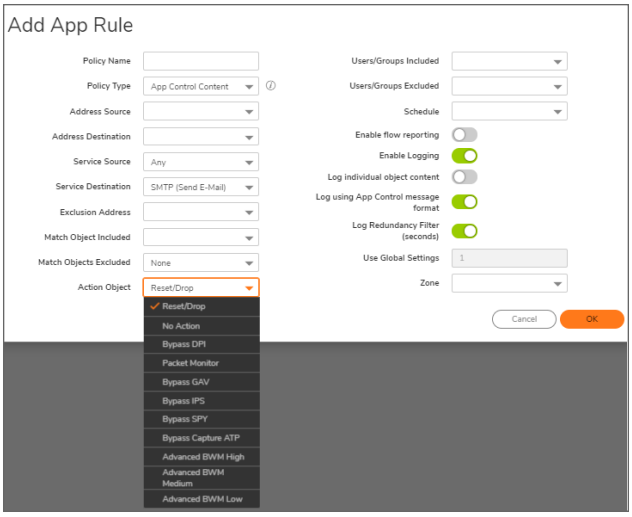
The default Action Objects include:

- BWM action objects

  The BWM action object options change depending on the Bandwidth Management Type setting on the **OBJECT | Profile Objects > Bandwidth** page. For more information about BWM actions, refer to Actions Using Bandwidth Management.

- Bypass action objects

  Bypass action objects are available if the indicated security services are licensed on the firewall.



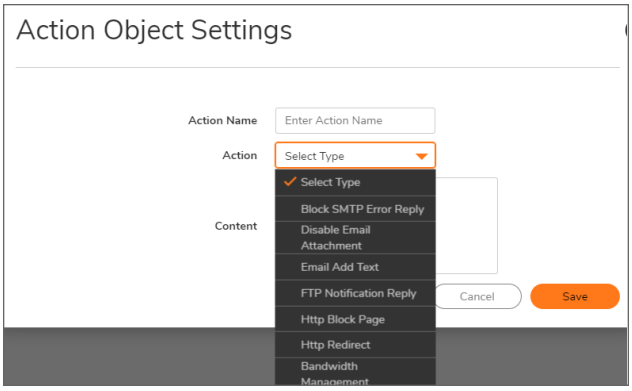
DEFAULT ACTION OBJECTS

Action Type	Description
Reset / Drop	Resets the connection for TCP and drops the packet for UDP.
No Action	Specifies policies without any action. This allows **log only** policy types.
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware, and application control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel. ⓘ **NOTE:** Bypass DPI does not stop filters that are enabled on the **NETWORK | Firewall > SSL Control** page.
Packet Monitor	• Captures the inbound and outbound packets in the session. • Copy the packets to another interface if mirroring is configured. The capture can be viewed and analyzed with Wireshark.
Advanced BWM High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum or burst bandwidth usage up to 100% of total available bandwidth, sets a priority of **one**.
Advanced BWM Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum or burst bandwidth usage up to 100% of total available bandwidth, sets a priority of **four**.
Advanced BWM Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum or burst bandwidth usage up to 100% of total available bandwidth, sets a priority of **six**.
Bypass GAV	Bypasses Gateway Anti-Virus inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass IPS	Bypasses Intrusion Prevention Service inspections of traffic matching the policy.
Bypass SPY	Bypasses Anti-Spyware inspections of traffic matching the policy.
Bypass Capture ATP	Provides a way to skip Capture Advanced Threat Protection (ATP) analysis in specific cases when you know the file is free of malware. This action persists for the duration of the entire connection as soon as it is triggered. ⓘ **NOTE:** Bypass Capture ATP does not prevent other anti-threat components, such as GAV and Cloud Anti-Virus, from examining the file.
Block SMTP E-Mail Without Reply	Blocks SMTP E-mail without reply.

Action Types for Custom Action Objects

You can create custom action objects for the **Action** types listed in the below table.

You can select a default or custom action object while adding or editing an app control policy on the **POLICY | Rules and Policies > App Rules** page.



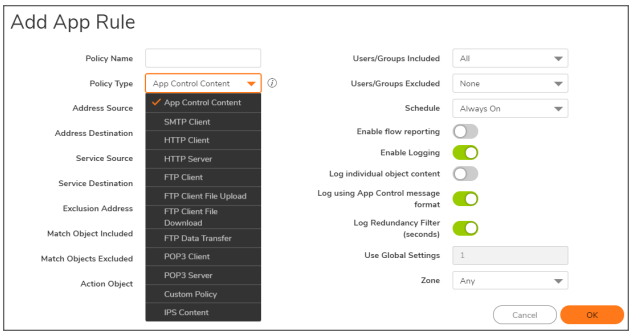
ACTION TYPES FOR CUSTOM ACTION OBJECTS

Action Type	Description
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.
Email - Add Text	Appends custom text at the end of the email.
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: *http://www.google.com*. If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.

NOTE: A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom *App Rules policies* using HTTP client, HTTP Server, Custom, and FTP file transfer types. For more information about policy types, refer to **About App Rules Policy Creation** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.



ⓘ **NOTE:** As a best practice, make sure that the Bandwidth Management profile settings are configured on the **OBJECT | Profile Objects > Bandwidth** page according to Configuring Bandwidth Profile Objects before configuring any BWM policies.

ACTION OBJECTS PAGE WITH BANDWIDTH MANAGEMENT TYPE

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. However, with *App Rules* you can specify all content type, which you cannot do with access rules.

Bandwidth management use cases:

- As an administrator you might want to limit .mp3 and executable file downloads during work hours to not more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth or even give the highest possible priority to downloads of the productive content.
- As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

A number of BWM action options are also available in the default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **OBJECT | Profile Objects > Bandwidth** page. For more information about bandwidth action objects, refer to Defining Bandwidth Profile Object Settings.

You can also create custom BWM actions according to Configuring Bandwidth App Rule Action Objects.

ⓘ **NOTE:** Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

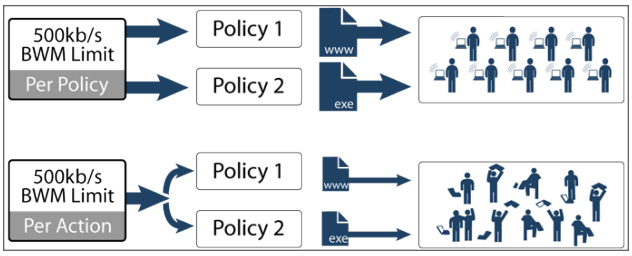
Topics:

- Bandwidth Management Methods
- Viewing Bandwidth Management Information on App Rule Actions

Bandwidth Management Methods

The Bandwidth Management feature can be implemented in the following ways.

BANDWIDTH MANAGEMENT: IMPLEMENTATION METHODS

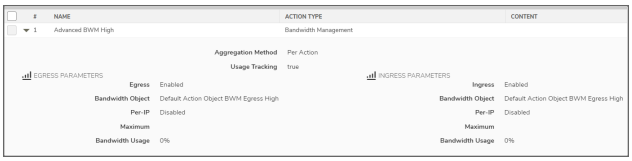


Aggregation Method	Description	Example
Per Policy	The bandwidth limit specified in a policy is applied individually to each policy.	Two policies each have an independent limit of 500 kb/s, the total possible bandwidth between those two rules is 1000 kb/s.
Per Action	The bandwidth limit action is applied (shared) across all policies to which it is applied.	Two policies share a BWM limit of 500 kb/s, limiting the total bandwidth between the two policies to 500 kb/s.

Viewing Bandwidth Management Information on App Rule Actions

To view bandwidth management information on App rule action object:

1. Navigate to **OBJECT | Action Objects > App Rule Actions**.
2. Click on the triangle icon for the App Rule Object.
   The Bandwidth Management details are displayed.



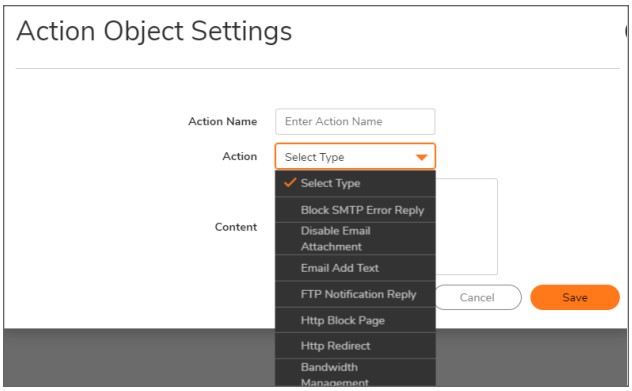
Adding Action Objects

NOTE: SonicOS has a number of default action objects as described in Default Action Objects. These action objects cannot be modified or deleted.

If you do not want to use one of the default actions, you can configure an Action Object. You can customize a configurable action with text or a URL for the **Action** types listed in Action Types for Custom Action Objects. The default action objects along with custom action objects are available for selection while adding an App Rule policy on **POLICY | Rules and Policies > App Rules > Add App Rule** page.

To add an Action Object:

1. Navigate to **OBJECT | Action Objects > App Rule Actions**.
2. Click the **Add** icon.
3. Enter a descriptive **Action Name**.
4. Select the **Action** type from the drop-down menu. For more information, refer to Action Types for Custom Action Objects.



5. Enter the text or URL to be used for the action in the **Content** field except for Actions, **HTTP Block Page** and **Bandwidth Management**.

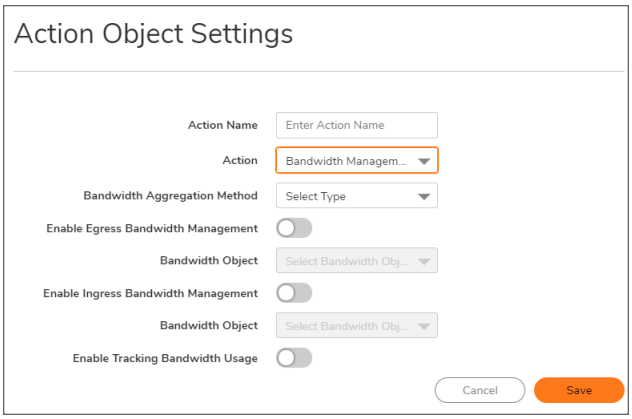
Action	Description
HTTP Block Page	1. Enter **Content** to be displayed when a page is blocked. 2. Select a background **Color** for the block page. 3. Click **Preview** to preview the block page message.
Bandwidth Management	Refer to Configuring Bandwidth App Rule Action Objects.

6. Click **Save**.
7. Click **Cancel** to go back to **App Rule Actions** page.

Configuring Bandwidth App Rule Action Objects

To configure a bandwidth action object:

1. Navigate to **OBJECT | Action Objects > App Rule Actions**.
2. Click the **Add** icon.
3. Enter a descriptive **Action Name**.
4. Select the **Action** as **Bandwidth Management** from the drop-down menu.



5. Select the **Bandwidth Aggregation Method** to be applied to the BWM object. For more information, refer to Bandwidth Management Methods.
   - Per Policy (default)
   - Per Action
6. Set the Bandwidth options.

Option	Description
Enable Egress Bandwidth Management	To enable BWM on outbound traffic
Enable Ingress Bandwidth Management	To enable BWM on inbound traffic

   Respective **Bandwidth Object** drop-down menu becomes active when the option is enabled.
7. Select **Bandwidth Object** from respective drop-down menu.
   - An existing BWM object
   - Create a new Bandwidth Object. For more information about creating a new bandwidth object, refer to Defining Bandwidth Profile Object Settings.
8. **Enable Tracking Bandwidth Usage** option to track bandwidth usage.

   ⓘ **NOTE:** You can enable the **Enable Tracking Bandwidth Usage** option only when the **Enable Egress Bandwidth Management** and/or **Enable Ingress Bandwidth Management** is selected.
9. Click **Save**.

Editing Action Objects

ⓘ | **NOTE:** You cannot edit the default Action Objects.

To edit an Action Object:

1. Navigate to **OBJECT | Action Objects > App Rule Actions**.
2. Hover over the action object to be edited and click the **Edit** icon.
3. Make the necessary changes.
   For more information, refer to Adding Action Objects.
4. Click **Save**.

Deleting Action Objects

ⓘ **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete custom Action Objects:

1. Navigate to **OBJECT | Action Objects > App Rule Actions**.
2. Do one of the following:
   a. Hover over the action object to be deleted and click the **Delete** icon.
   b. Select check boxes of the action objects to be deleted and click the **Delete** icon on top of the table.
   c. Select the check box in the table header to select all custom action objects and click the **Delete** icon on top of the table.
3. Click the **Confirm** in the confirmation dialog box.

Applying App Rule Actions

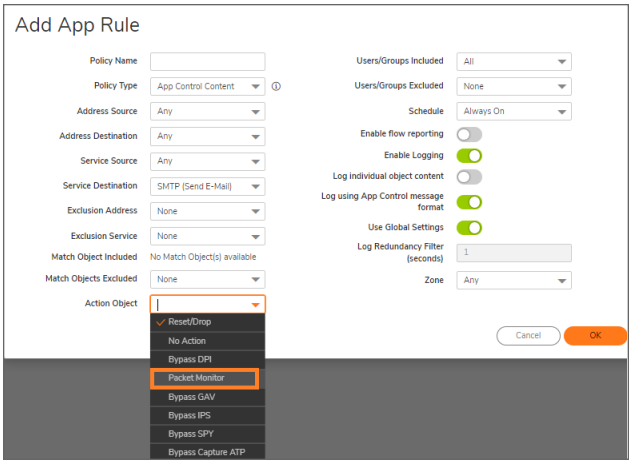
Once the **App Rule Actions** are created, you can apply them in App Rules Policy on **POLICY | Rules and Policies > App Rules** page. For more information, refer to **Configuring an App Rules Policy** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

Topics:

Related Tasks for Actions Using Packet Monitoring

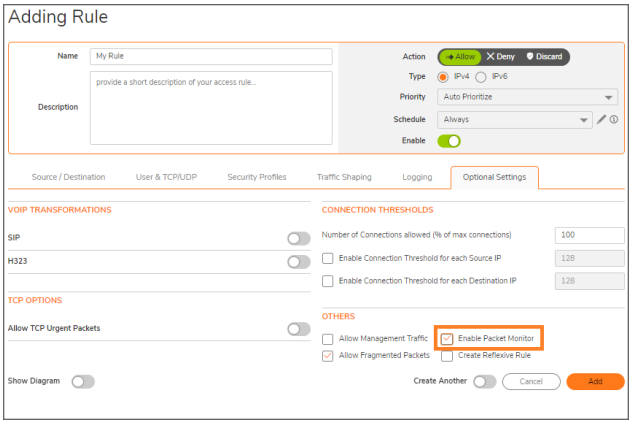
Packet Monitor takes a deeper look at application traffic. SonicOS captures or mirrors the traffic according to the settings you have configured on the **MONITOR | Tools & Monitors > Packet Monitor** page, when:

- App Rules policies created on **POLICY | Rules and Policies> App Rules** page use an action object with Packet Monitor action type.



- Access Rules policies created on the **POLICY | Rules and policies > Access Rules** page that use

Packet Monitor.



The default is to create a capture file, which you can view with Wireshark™. For more information, refer to Wireshark.

Topics:

- Capturing Packets Related to a Policy
- Configuring Mirroring

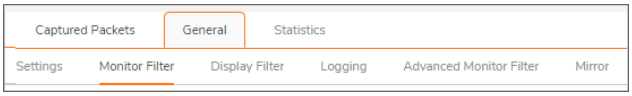
Capturing Packets Related to a Policy

ⓘ **NOTE:** Make sure that at least one rule is configured from the below list:

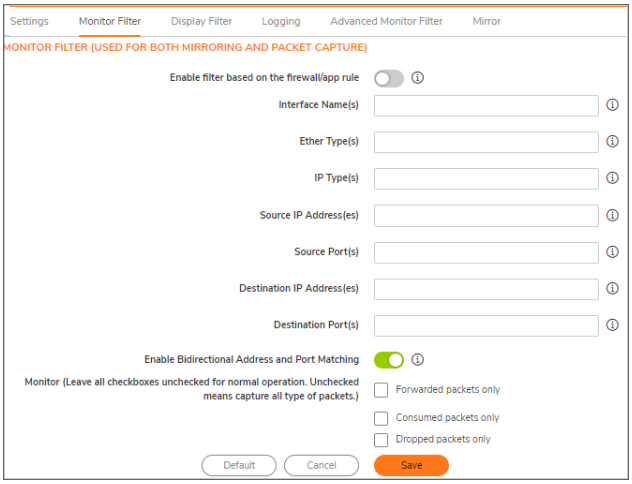
- An App Rules policy with the Packet Monitor as an Action Object.
- An Access Rules policy that uses Packet Monitor.

To control the Packet Monitor action to capture only the packets related to your policy:

1. Navigate to **MONITOR | Tools & Monitors > Packet Monitor > General**.

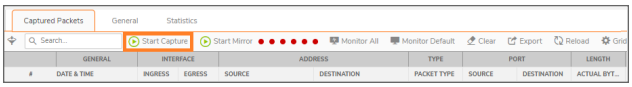


2. Click **Monitor Filter** tab.



3. Select **Enable Filter based on the firewall/app rule** to filter the traffic based on the app rule or access rule policy.
4. Click **Save**.
5. Navigate to **Capture Packets** tab and click **Start Capture**.

   Packets are not captured until some traffic triggers an App Rules policy (or an Access Rule). You can see the Alert message in the **MONITOR | Logs > System Event** page when the policy is triggered.
6. Click **Stop Capture** after you have captured the desired packets.

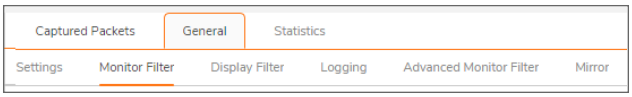


You can Export the capture into different formats and look at it in a browser.

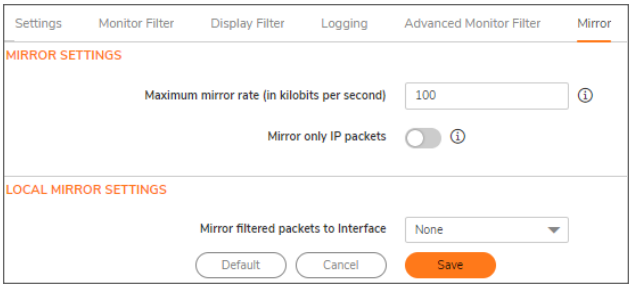
Configuring Mirroring

To set up mirroring:

1. Navigate to **MONITOR | Tools & Monitors > Packet Monitor > General**.



2. Click **Mirror** tab.



3. Pick an interface to which to send the mirrored traffic from the **Mirror filtered packets to Interface** drop-down menu under **Local Mirroring Settings**.

   You can also configure one of the **Remote** settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture MSN Instant Messenger traffic and read the conversations.

4. Click **Save**.

2

Content Filter Actions

SonicOS Content Filtering Service (CFS) delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites that students and employees can access using their IT-issued computers while behind the organization's firewall.

For information about upgrading from an older version to CFS 4.0, refer to the SonicWall Content Filtering Service Upgrade Guide.

Topics:

Content Filter Objects

ⓘ | **NOTE:** You cannot edit or delete the **CFS Default Action** and **CFS Default Profile** objects.

Content Filtering Service (CFS) uses secure objects for filtering content. For more information about the secure objects and their use, refer to SonicOS Secure Objects section in SonicOS 7.0 System Administration Guide.

You can also configure the Passphrase and Confirm (Consent) features within content filter objects.

Feature	Description
Passphrase	Restricts web access unless the user enters the correct passphrase or password. For more information, refer to About Passphrase Feature.
Confirm	Restricts web access unless the user confirms that they want to proceed to the website. For more information, refer to About Confirm Feature.

CFS uses the Action Objects for content filtering. For more information, refer to CFS Action Objects.

SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) for all types of Content Filter objects during their creation. For more information, refer to UUIDs for CFS Objects.

Topics:

CFS Action Objects

The CFS Action Object defines an action after a packet is filtered by CFS and matches a CFS policy.

About Passphrase Feature

The Passphrase feature, in conjunction with the About Confirm Feature, restricts web access based on a passphrase or password. You can configure the passphrase operation for special URI categories or domains in the Forbidden URI List. To access the forbidden URIs, users are asked to enter the correct password or else web access is blocked.

ⓘ **IMPORTANT:** Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

How the Passphrase operation works:

1. The user attempts to access a restricted website.
2. A Passphrase page displays on the user's browser.
3. The user must enter the passphrase or password and submit it.
4. CFS validates the submitted passphrase or password with the website's password:
   - If the passphrase or password matches, web access is allowed. No further confirmations are needed and users can continue to access websites of the same category for the Active Time period set for the Confirm feature. The default is 60 minutes.
   - If the passphrase or password does not match, access is blocked, and a Block page is sent to the user.

     ⓘ **NOTE:** Users have three chances to enter the correct passphrase or password. The site is blocked if all chances fail.

   If the user selects **Cancel**, the site is blocked immediately.

About Confirm Feature

The Confirm feature (also known as Consent) restricts web access by requiring a confirmation from the user before allowing access. You can configure the Confirm operation for special URL categories or domains, and the users need to confirm the web request when they first visit the sites.

IMPORTANT: Confirm only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (Consent) page.

How the Confirm operation works:

1. The user attempts to access a blocked website.
2. A pop-up dialog box appears, requesting confirmation.
3. Users must select **Continue** or **Close**.
    - If a user **Continue** to confirm access this category of websites, user is redirected to the first confirmed website. No further confirmations are needed and users can continue to access websites of the same category for the Active Time period that is set for the Confirm feature. The default is 60 minutes.
    - If a user chooses **Close**, user is shown the Block page and is blocked from that category of website for the period of the Active Time setting.

UUIDs for CFS Objects

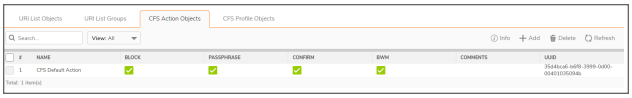
SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) for these Content Filter objects and groups during their creation:

- URI List Object
- URI List Group
- CFS Action Object
- CFS Profile Object

SonicOS also generates and binds UUIDs to Content Filter Policies during creation. A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of an object and remains the same thereafter, even when the object is modified or after rebooting the firewall. The UUID is removed when the object is deleted and cannot be reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

By the default, UUIDs are not displayed in the table. You can customize the table columns to show the UUID column. For more information, refer to Common Actions with Objects Table.

When displayed, UUIDs appear in the CFS object tables for each object or group type.



CFS object UUIDs facilitate the following functions:

- You can search for a CFS object by UUID with the global search function of the management interface.
- You can display the reference count and referring entity by hovering over the balloon on the CFS objects if an object with a UUID is referenced by another entity with a UUID.

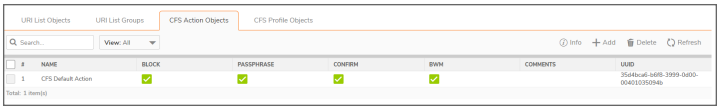
When a CFS Action Object, CFS Profile Object, URI List Object, or URI List Group is used by a Content Filter Policy, you can display the reference count and referenced policy by hovering over the balloon in the Comment column on the object's page under **Object**.

Managing CFS Action Objects

Topics:

- About the CFS Action Objects Table
- Adding CFS Action Objects
- Editing CFS Action Objects
- Deleting CFS Action Objects

About the CFS Action Objects Table



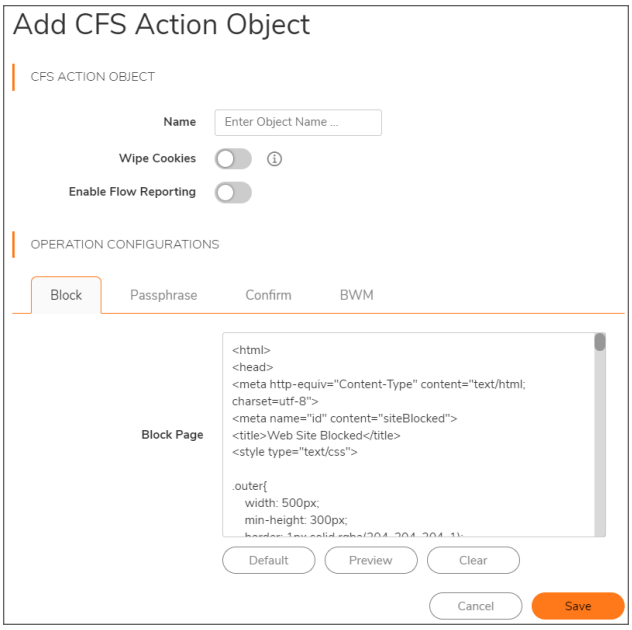
Name	Name of the CFS Action Object. Name of the default CFS Action Object is **CFS Default Action**. The default object can be edited, but not deleted.
Block	Indicates whether a block page has been configured.
Passphrase	Indicates whether a passphrase page has been configured.
Confirm	Indicates whether a confirm page has been configured.
BWM	Indicates whether bandwidth management has been configured.
Comments	Contains comments added during the creation of CFS Action Objects.
UUID	Contains automatically generated UUIDs (Universally Unique Identifiers) for the Content Filter objects and groups.

Adding CFS Action Objects

ⓘ **NOTE:** A default CFS Action Object, **CFS Default Action**, is created by SonicOS. You can configure and edit the default CFS Action Object, but you cannot delete it.

To add a CFS Action Object:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click the **Add** icon.



3. Enter a **Name** of the CFS Action Object.
4. Enable the **Wipe Cookies** to remove the cookies automatically to protect privacy.

   Cookies for HTTPS sites are removed only when both the **Wipe Cookies** and **Client DPI-SSL Content Filter** are enabled.

   ⓘ **IMPORTANT:** Enabling the **Wipe Cookies** option may break the Safe Search Enforcement function for some search engines.
5. **Enable Flow Reporting** to send URI information to the AppFlow Monitor.
6. Configure the following pages, as required, to display when a site is blocked:

   ⓘ **NOTE:** A default version is available for each of these pages. You can either modify the default page to meet your requirements or create a new page.

Block	To configure a blocked site according to company policy
Passphrase	To configure a password-protected web page
Confirm	To configure a restricted web page that requires confirmation to access

7. Allocate bandwidth resources as a part of CFS Action Objects.
   For more information, refer to BWM.
8. Click **Save**.
   The new CFS Action Object is added to the CFS Action Object table.

Block

From the **Block** option, you can configure a blocked page according to company policy. A default version is available for Block page. You can either modify the default page to meet your requirements or create a new page.

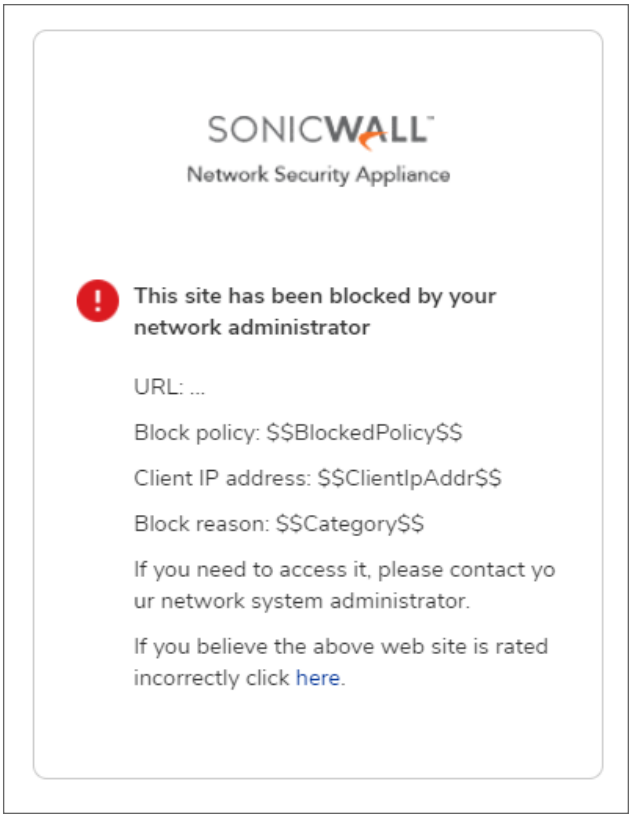
To create a block page:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click the **Add** icon.
3. Click the **Block** tab under **OPERATION CONFIGURATIONS** group.

4. Do one of the following:
   a. No action is required to continue with the default web page.
   b. Make the necessary changes to the default code if you want to customize the web page.
   c. Click **Clear** and enter your own code for a new web page.

5. Click **Preview** to preview the web page.

   If you continue with the default web page, the Block policy, Client IP address, and the reason for the block are shown in the preview.



6. Click **Return** icon to go back to CFS Action Object page.
7. Click **Default** if you wish to continue with the default blocked page.
8. Click **Save**.

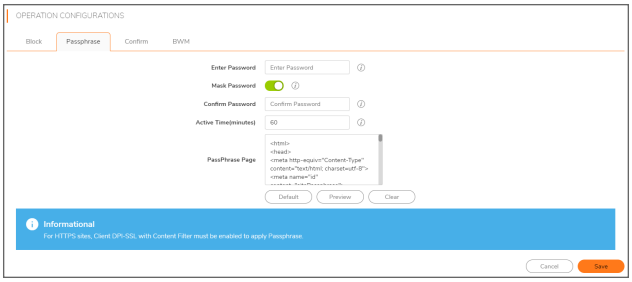
ⓘ **NOTE:** This option can be applied in Adding CFS Profile Objectson **OBJECT | Profile Objects > Content Filter** page.

Passphrase

NOTE: For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Passphrase. For more information, refer to About Passphrase Feature.

To create a password-protected web page:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click the **Add** icon.
3. Click the **Passphrase** tab under **OPERATION CONFIGURATIONS** group.



4. Enter the passphrase or password for the website in the **Enter Password** field. The password can be up to 64 characters.

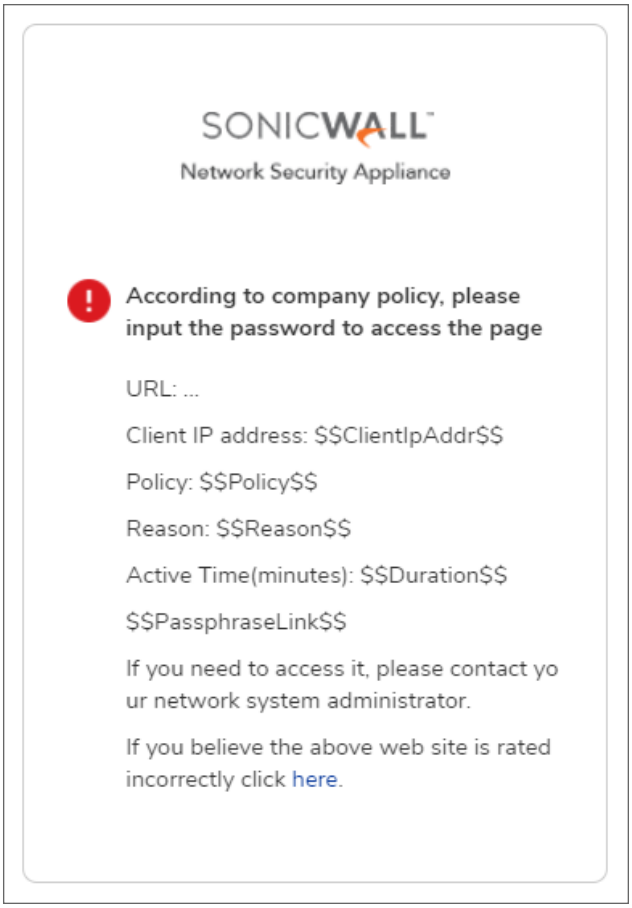
   NOTE: The **Mask Password** option is enabled by the default. Disabling this option converts the password into plain text and the entry in the **Confirm Password** field becomes visible.

5. Enter the same passphrase or password again in the **Confirm Password** field.
6. Enter the effective duration, in minutes, for a passphrase based on category or domain in the **Active Time (minutes)** field.

   The minimum time is 1, the maximum is 9999, and the default is **60**.

7. Do one of the following with **Passphrase Page** code:
   a. No action is required to continue with the default web page.
   b. Make the necessary changes to the default code if you want to customize the web page.
   c. Click **Clear** to enter your own code for a new web page.

8. Click **Preview** to preview the web page.



If you continue with the default web page, website URL, Client IP address, policy, reason, and active minutes along with a field for entering the password are shown in the preview.

9. Click **Return** icon to go back to CFS Action Object page.
10. Click **Default** if you wish to continue with the default blocked page.
11. Click **Save**.

ⓘ **NOTE:** This option can be applied in Adding CFS Profile Objectson **OBJECT | Profile Objects > Content Filter** page.

Confirm

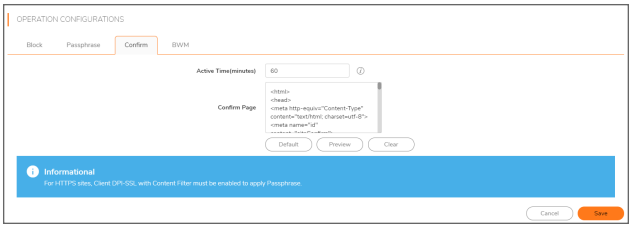
Confirm helps to build a restricted web page that requires the user confirmation to access.

ⓘ **NOTE:**

- Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page.
- For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Confirm. For more information, refer to About Confirm Feature.

To create a restricted web page that requires confirmation:

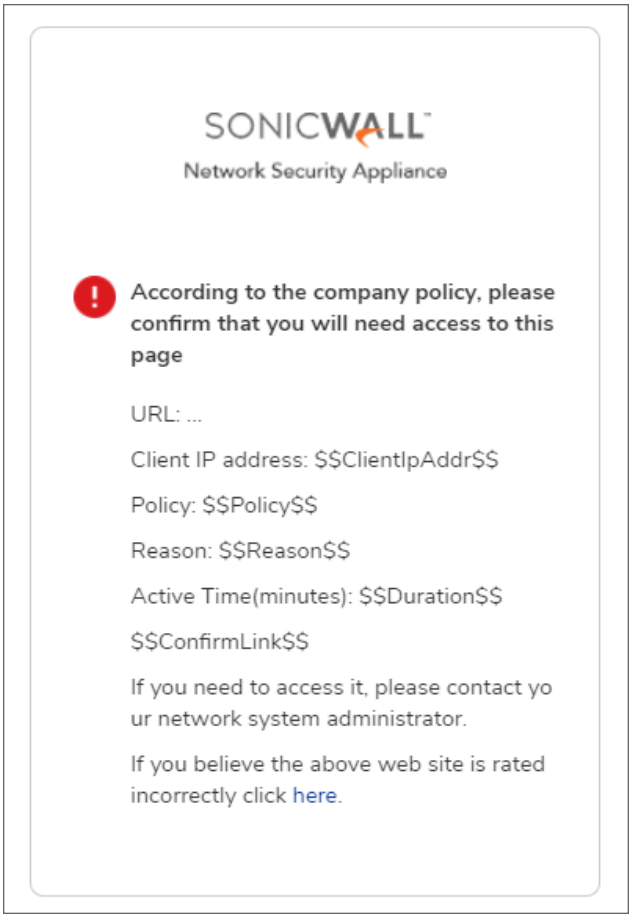
1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click the **Add** icon.
3. Click the **Confirm** tab under **OPERATION CONFIGURATIONS** group.



4. Enter the effective duration, in minutes, for a confirmed user based on category or domain in the **Active Time (minutes)** field.
   The minimum time is 1, the maximum is 9999, and the default is **60**.
5. Do one of the following with **Confirm Page** code:
   a. No action is required to continue with the default web page.
   b. Make the necessary changes to the default code if you want to customize the web page.
   c. Click **Clear** and enter your own code for a new web page.

6. Click **Preview** to preview the web page.

   If you continue with the default web page, web site URL, Client IP address, policy, reason for the block, and active minutes along with a field for entering the confirmation are shown in the preview.



7. Click **Return** icon to go back to CFS Action Object page.
8. Click **Default** if you wish to continue with the default blocked page.
9. Click **Save**.

ⓘ **NOTE:** This option can be applied in Adding CFS Profile Objectson **OBJECT | Profile Objects > Content Filter** page.

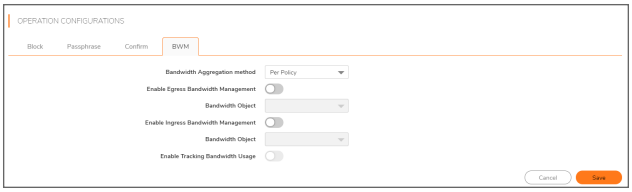
BWM

IMPORTANT: CFS Bandwidth Action Objects are similar to, but not the same as, Bandwidth Profile Objects created on the **OBJECT | Profile Objects > Bandwidth** page. CFS BWM Action Objects do not appear on the **OBJECT | Profile Objects > Bandwidth** page and BWM profile objects do not appear on the **OBJECT | Action Objects > Content Filter Actions** page. But, you can use the BWM Profile Objects created on the **OBJECT | Profile Objects > Bandwidth** page to configure a CFS BWM Action Object.

NOTE: For more information about bandwidth management, refer to the Actions Using Bandwidth Management.

To allocate bandwidth resources for content filtering:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Click the **Add** icon.
3. Click the **BWM** tab under **OPERATION CONFIGURATIONS** group.



4. Select the **Bandwidth Aggregation Method** to be applied to the BWM object. For more information, refer to Bandwidth Management Methods.
   - Per Policy (default)
   - Per Action
5. Set the Bandwidth options.

Option	Description
Enable Egress Bandwidth Management	To enable BWM on outbound traffic
Enable Ingress Bandwidth Management	To enable BWM on inbound traffic

   Respective **Bandwidth Object** drop-down menu becomes active when the option is enabled.
6. Select **Bandwidth Object** from respective drop-down menu.
   - An existing BWM object
   - Create a new Bandwidth Object. For more information about creating a new bandwidth object, refer to Defining Bandwidth Profile Object Settings.
7. **Enable Tracking Bandwidth Usage** option to track bandwidth usage.

   NOTE: You can enable the **Enable Tracking Bandwidth Usage** option only when the **Enable Egress Bandwidth Management** and/or **Enable Ingress Bandwidth Management** is selected.
8. Click **Save**.

Editing CFS Action Objects

To edit a CFS Action Object:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Hover over the CFS Action Object to be edited and click the **Edit** icon.
3. Make the necessary changes. For more information, refer to Adding CFS Action Objects.
   You cannot change **Name** of the CFS Default Action object.
4. Click **Save**.

Deleting CFS Action Objects

ⓘ **NOTE:**

- You cannot delete the default items.
- Check boxes of the default items in the table are unavailable for selection.
- You cannot delete an item if it is in use by Rule.
- You can delete only custom items.

To delete custom CFS Action Objects:

1. Navigate to **OBJECT | Action Objects > Content Filter Actions**.
2. Do one of the following:
   a. Hover over the CFS Action Object to be deleted and click the **Delete** icon.
   b. Select check boxes of the CFS Action Objects to be deleted and click the **Delete** icon on top of the table.
   c. Select the check box in the table header to select all CFS Action Objects and click the **Delete** icon on top of the table.
3. Click **Confirm** in the confirmation dialog box.

Applying Content Filter Objects

Once the Content Filter Objects are created, you can apply them in configuring content filter rules on **POLICY | Rules and Policies > Content Filter Rules** page. For more information, refer to **Adding a Content Filter Rule** section in SonicOS 7.0 Rules and Policies Administration Guide for Classic Mode.

Make sure that Content Filters is configured on the **POLICY | Security Services > Content Filter** page to make the CFS into action. For more information, refer to **Configuring Content Filter** section in SonicOS 7.0 Security Services Administration Guide.

OBJECT VIEWER

Object Viewer feature is available only in Policy Mode at left bottom corner of the left navigation menu. You can access the Object Viewer across all the screens. For example, you can access the Object Viewer even if you are on the POLICY page.

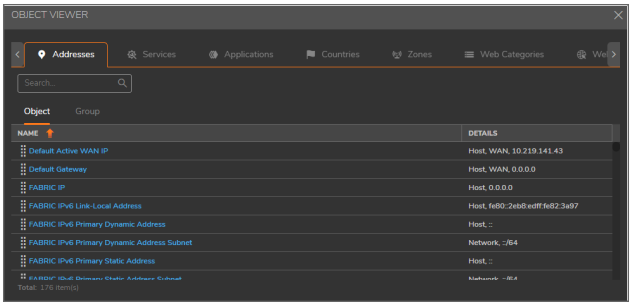
Object Viewer is one place solution to find all the objects, match objects, profile objects, and action profiles created in your account. Use the below listed icons to manage the Object Viewer.

Icon	Use this Icon
	To drag and drop the Object Viewer on to the screen anywhere.
	To show or hide the Object Viewer details in the left navigation menu.
	To expand the Object Viewer on to the screen and move anywhere on the screen.
	To minimize the Object Viewer to the left navigation menu.
	To get the latest object details in the Object Viewer.

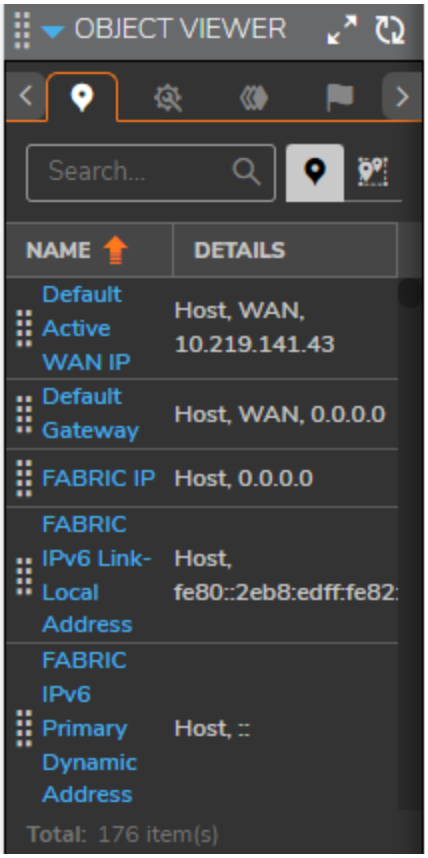
Searching for an object:

You can search with a keyword in the field under respective object if you are looking for any specific object. Below are the maximized and minimized views of the Object Viewer.

Maximized Object Viewer:



Minimized Object Viewer :



6

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS ObjectsAdministration Guide
Updated - June 2024
Software Version - 7.0
232-006112-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-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