Secure Mobile Access 12.4.3

Administration Guide

SONICWALL®

Contents

1

Introduction

About Secure Mobile Access

Topics:

Secure Mobile Access on SMA Appliances

Welcome to the *Secure Mobile Access 12.4.3* Administration Guide. This manual provides the information you need to successfully activate, configure, and administer Secure Mobile Access (SMA) on SonicWall SMA appliances.

SonicWall SMA appliances provide secure access-including clientless access to web applications, access to client/server applications, and file sharing-to employees, business partners, and customers. All traffic is encrypted using Secure Sockets Layer (SSL) to protect it from unauthorized users.

The appliance makes applications available from a range of access methods-including a standard Web browser, a client application (example, Connect Tunnel), or a mobile device app-on a wide range of platforms including Windows, MacOS, Linux, and mobile devices.

You might use the appliance to create a:

- Remote access VPN that enables remote employees to securely access private company applications such as email over the Internet.
- Business partner VPN that provides designated suppliers with access to an internal supply chain application over the Internet.

The appliance's granular access control lets you define policy and control access down to the user and resource level. Managing policy and configuring the appliance is quick and easy with the Web-based management console.

For an overview of planning your SonicWall Secure Mobile Access appliance configuration and deployment, see the *Secure Mobile Access Deployment Planning Guide*.

ⓘ | **IMPORTANT:**

- You can directly upgrade to SMA 12.4.3 from SMA 12.1.0 version with latest hotfixes.
- You can directly upgrade to SMA 12.4.3 from SMA 12.4.1 version.
- You can directly upgrade to SMA 12.4.3 from SMA 12.4.2 version with latest hotfixes.

ⓘ | **IMPORTANT:** When you are upgrading from SMA 12.3, it is recommended to upgrade to 12.4.1 first, then upgrade to 12.4.3.

About SMA Documentation

Your SonicWall SMA appliance also comes with a printed *Getting Started Guide*, and there is a *SonicWall SMA Deployment Planning Guide* that explains important VPN concepts and components and aids in deploying your VPN. For access to electronic copies of all product documentation, visit the SonicWall Support portal or log in to your MySonicWall account and register your appliance. See Registering Your SMA Appliance for more information.

Document Conventions

Throughout this document:

- External refers to the network interface connected to the Internet.
- Internal refers to the network interface connected to your internal corporate network.

This document uses the following typographical conventions:

DOCUMENT CONVENTIONS

Typographical convention	Usage
Bold	User interface components (such as UI page(s), text fields, or buttons).
`Monospace font`	Information you are supposed to type.
`commandname -x [-y]`	In command-line syntax, square brackets indicate optional parameters.

What’s New in This Release

SonicWall Secure Mobile Access (SMA) 12.4.3 includes these new features:

Topics:

- Cisco Duo Security Multi-factor Authentication Server
- RSA SecurID Authentication Manager
- Dynamic Form SSO Improvements
- Exclusions
- Supportability Enhancements

Cisco Duo Security Multi-factor Authentication Server

Cisco Duo Security Multi-factor Authentication (MFA) Server is a popular cloud service that provides multi-factor authentication as service to other applications. This service offers push notification, phone call, SMS among other factors of authentication. You can use Cisco Duo Security to authenticate users.

Cisco Duo Security Multi-Factor Authentication servers are supported by all the actively supported clients like Connect Tunnel (CT) on Windows/Mac/Linux platforms, and Workplace.

Refer to the Integration of SMA with Cisco Duo Security MFA Server section.

RSA SecurID Authentication Manager

RSA SecurID Authentication Manager is a widely used solution for multi-factor authentication (MFA). It provides an additional layer of security by requiring users to authenticate with password or token or application generated codes.

The Authentication Manager is the central component that manages security tokens, users, multiple applications, agents, and resources across physical sites, and to help secure access to network, Cloud, and web-accessible applications to enhance security.

From SMA1000 12.4.3 onwards RSA SecurID Authentication Manager is integrated with SMA1000 which acts as an agent to RSA Authentication Manager and leverages its authentication services.

Refer to the Integration of SMA1000 with RSA SecurID Authentication Manager section.

Dynamic Form SSO Improvements

Dynamic Form SSO allows users to login to their web applications automatically without requiring them to manually enter the credentials. The profile configuration involves providing the attributes of HTML Forms that are used by end-user to log in to web-application. Dynamic SSO is to login the user automatically whenever login page is displayed.

In SMA1000 12.4.3 a new login experience is provided where admin can choose SSO or login behavior based on the resource application.

- New option **Login experience** is available to configure how the user will be automatically logged in.
- New login detection method **Status code** is added.

Refer to the Creating Forms-Based Dynamic Single Sign-On Profiles section.

Exclusions

Use exclusions to prevent any resources (including host names, IP addresses, or domains) from being redirected through the appliance. When specifying a domain, you can also use the wildcard characters asterisk (*) and question mark (?).

In SMA1000 12.4.3 AMC:

- Allows tunnel configurations with redirect-all and wildcard domain exclusions.
- Connect Tunnel clients are capable of excluding the traffic on the fly.

Refer to the Using the Exclusions and Selecting Tunnel Access Methods for a Community sections.

Supportability Enhancements

In SMA1000 12.4.3, the following are the Supportability Enhancements.

Topics:

- Always On VPN Enhancements
- Device VPN Enhancements
- Configuring Cached Credentials
- Configuring Global Overrides in AMC
- Downloading the SMA1000 Client Installation Packages
- Managing Administrator Account Settings
- Configuring Access Request Logging
- Configuring Shell Access
- Copying Resources Groups

Always On VPN Enhancements

Always On VPN enforces that a VPN connection is always active during the Windows user session. When **Always On VPN** is enabled, a VPN connection is established automatically between the user's device and the SMA1000 appliance whenever the device has a network connection to the internet.

Once the Connect Tunnel is installed with **Always On VPN** enabled, a VPN connection is established. When the client and system restarts after a network change or system hibernation, both the client and system gets locked down, preventing users from disconnecting the VPN or accessing the internet without VPN.

In SMA1000 12.4.3, admin has the ability to provide internet access to users even if the VPN gets disconnected. Additionally, the admin can now control whether a user is allowed to disconnect from the VPN. This can be achieved with the following options:

- **Allow user to disconnect**
- **Restrict network access when VPN is not Connected**

Refer to the Selecting Tunnel Access Methods for a Community section.

Device VPN Enhancements

Device VPN provides VPN access to user devices when a user is not logged in. Device VPN is supported on Windows using the Connect Tunnel client.

In SMA1000 12.4.3, the **Device VPN Communities** (under **Services > Network Tunnel Service**) has two additional check boxes that allows users to bypass entering VPN credentials for User VPN, when the client machine is powered on or restarts in secure network. Also, if Device VPN is enabled, **Allow user to disconnect** option takes precedence over **Always On VPN** configuration. Below are the two Device VPN options:

- **Allow user to disconnect**
- **Do not connect on secure network**

Refer to the Configuring Device VPN section.

Configuring Cached Credentials

In SMA1000 12.4.3, two more ways to use cached credentials are provided.

- **Username only**
- **Disabled**

Refer to the Selecting Tunnel Access Methods for a Community section.

Configuring Global Overrides in AMC

In SMA100012.4.3, the **Enable accounting records** value for realms can now be overridden when set to different options accordingly under **Global Overrides**.

Refer to the Configuring Global Overrides in AMC section.

Downloading the SMA1000 Client Installation Packages

This section describes how to download the installation package for the Connect Tunnel client to your local workstation.

In SMA1000 12.4.3, ensure that the latest processor and versions are supported to download the client:

- ARM 64 processor is supported for Windows and Linux.
- MacOS Big Sur (11.x) apple version is required for MAC operating system.

Refer to the Downloading the Secure Mobile Access Client Installation Packages section.

Managing Administrator Account Settings

Secure Mobile Access allows you to choose the authentication server where your appliance administrators are defined.

In SMA100012.4.3 **Advanced** tab provides the following:

- **Password Policy** settings help to set strong password complexity settings for the primary administrator account.
- **Account lockout** settings for administrators when there are multiple failed login attempts.
- **Session timeout** settings for administrators to configure the session inactivity timeout.
- **Concurrent Session** settings for administrators to configure the concurrent session to limit the number of sessions and admins that can be logged in to AMC.

Refer to the Managing Administrator Account Settings section.

Configuring Access Request Logging

In SMA100012.4.3 you can limit the types of access requests that are saved with User Sessions.

Refer to the Configuring Access Request Logging section.

Configuring Shell Access

In SMA100012.4.3 configuring **Shell Access** settings allows to configure the shell access settings to allow or prevent all shell access via the serial console and SSH. By default the Shell access is always enabled.

Refer to the Enabling SSH Access from Remote Hosts section.

Copying Resources Groups

In SMA100012.4.3, rather than creating a new resource group from scratch, you can save time by making a copy of an existing group and changing some parameters to fit the new group. Refer to the Editing, Deleting and Copying Resource Groups section.

Discontinued Features

Discontinued features in SMA1000 12.4.1 onwards are:

- vWorkspace
- Fallback Servers

- Application Control

Discontinued features in SMA1000 12.4.3 onwards are:

- RSA ClearTrust
- Modern Workplace
- Cache Cleaner
  - ⓘ | **NOTE:** When upgrading the SMA version with discontinued features, it is mandatory to remove the existing configuration and then proceed with the upgrade.

Deprecated Features

These features are deprecated on all SMA appliances in SMA 12.4:

Legacy SSO	Legacy SSO is deprecated and enhanced with Dynamic Single Sign On feature.
RSA Authentication Manager (Legacy)	RSA Authentication Manager (Legacy) is deprecated and enhance with latest RSA SecurID Authentication Manager.

Features of Your SMA Appliance

Topics:

- SonicWall SMA Appliance Models
- Administrator Components for Managing Appliances and Services
- User Access Components
- Related Documentation

SonicWall SMA Appliance Models

SonicWall offers the following SMA series appliance models, all of which are documented in this manual. In this document, the term “SMA appliance” refers to the appliances listed in the below table.

SMA APPLIANCE MODELS

This appliance	Supports up to this many concurrent users
SMA 7200	10000
SMA 7210	10000
SMA 6200	2000
SMA 6210	2000
SMA 8200v Virtual Appliance	5,000 users for Hyper-V, ESXi, AWS, Azure, and KVM

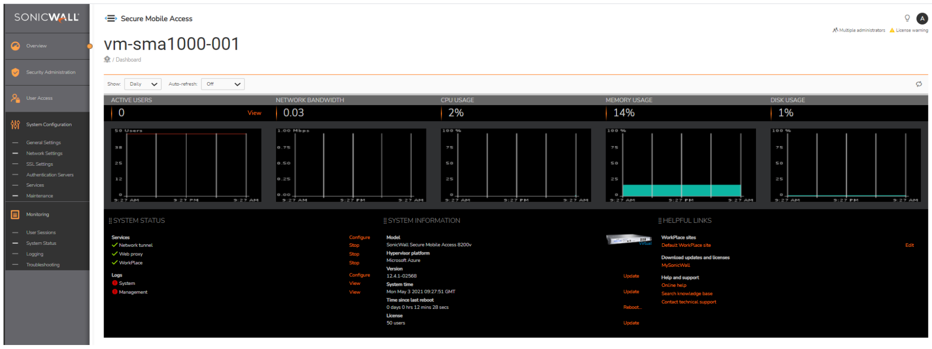
ⓘ | **NOTE:** SMA 12.4.2 is not supported on the EX6000, EX7000, and EX9000 appliances.

Administrator Components for Managing Appliances and Services

- **Appliance Management Console (AMC)** is a Web-based administrative tool (see AMC Dashboard) that manages the appliance by providing centralized access for:
  - Managing security policies
  - Configuring the system (including networking and certificate configuration)
  - Monitoring

  AMC is accessible from a Web browser.

  ### AMC DASHBOARD



vm-sma1000-001

Show: Daily Auto-refresh: Off

ACTIVE USERS	NETWORK BANDWIDTH	CPU USAGE	MEMORY USAGE	DISK USAGE
0	0.03	2%	14%	1%

SYSTEM STATUS

Services
✓ Network tunnel
✓ Web proxy
✓ WorkPlace

Logs
● System
● Management

SYSTEM INFORMATION

Model
SonicWall Secure Mobile Access 8200v
Hypervisor platform
Microsoft Azure
Version
12.4.1-02568
System time
Mon May 3 2021 09:27:51 GMT
Time since last reboot
0 days 0 hrs 12 mins 28 secs
License
50 users

HELPFUL LINKS

WorkPlace sites
Default WorkPlace site
Download updates and licenses
MySonicWall
Help and support
Online help
Search knowledge base
Contact technical support

- **Web proxy service** provides users with secure access to Web-based applications, Web servers, and network file servers from a Web browser. Web proxy service is a secure HTTP reverse proxy that brokers and encrypts access to Web-based resources.
- **Network tunnel service** is a network routing technology that provides secure network tunnel access to a wide range of applications, including those that use:
  - Non-TCP protocols such as Voice Over IP (VoIP) and ICMP
  - Reverse-connection protocols
  - Bi-directional protocols such as FTP

  Network tunnel service works in conjunction with the Connect Tunnel client, the OnDemand Tunnel agent, and the Mobile Connect client to provide authenticated and encrypted access. It can traverse firewalls, NAT devices, and other proxy servers that can interfere with traditional VPN devices.
- **Management API** provides RESTful API to view and modify appliance data in JSON format. The API is divided into two primary RESTful API that handle HTTP requests before and after the appliance has completed initial configuration:
  - During initial configuration: `https://`*`<AMC IP address:8443>`*`/Setup`
  - On configured appliance: `https://`*`<AMC IP address:8443>`*`/Console`

  where *`<AMC IP address>`* is the IP address of your SMA appliance.

  Browser-based documentation is available at:

- `https://<AMC IP address:8443>/Setup/Help`
- `https://<AMC IP address:8443>/Console/Help`

User Access Components

The SMA appliance includes several components that provide users with access to resources on your network:

- WorkPlace
- Connect and OnDemand Tunnel Clients
- Mobile Connect Clients
- End Point Control (EPC)

WorkPlace

The WorkPlace portal provides users with quick access to resources on your network. WorkPlace provides a range of access methods for you to choose from:

- Basic Web (HTTPS) resources are accessible using the Web translation engine, a reverse proxy that provides single sign-on and fine-grained access control. The web translation engine has three modes of operation:
  - **Alias**-based translation appends a custom alias to the end of the URL that users access (also called URL re-writing). For example, if you specify `http://hr.mycompany.com/` as a URL resource with an alias of hr, users would access it by clicking on a link in Workplace that looked like this: `https://vpn.mycompany.com/hr/`. This type of configuration is recommended for simple web applications that do not require advanced functionality, like JavaScript. SonicWall supports a limited number of applications in the alias-based translated web access method; see Web Application Services.
  - **Host-mapped URL** access changes the hostname that the resource is accessed on. For example, if `http://hr.mycompany.com/` URL resource is configured with a custom hostname of `hr.vpn.mycompany.com`, users access the resource by clicking on a link that looks like this in Workplace: `https://hr.vpn.mycompany.com/`. Host mapped URL access is recommended for complex web applications that may use advanced JavaScript (and other advanced web technologies).
    - **Port-mapped URL** access changes the port number that the resource is accessed on. For example, if `http://hr.mycompany.com/` URL resource is configured with a custom port (8888) for access, users access the resource by clicking on a link that looks like this in Workplace: `https://vpn.mycompany.com:8888/`. One of the downsides of custom port URL access is that it does require you to open up a port for each web application that you want to configure to use the port mapped URL access.

      ⓘ **TIP:** Port-mapped URL resources is recommended for complex web applications that may use JavaScript, and other advanced web technologies.
- File system resources are accessible from the Network Explorer that is integrated in WorkPlace.

- Client/server traffic (TCP/IP) is accessible using one of the network redirection clients, OnDemand Tunnel. The client is provisioned automatically or activated when the user logs in to WorkPlace.

The access method you choose will be based on several factors, including the network protocols used by your applications, your security requirements, end-user convenience, and the target platforms.

WorkPlace Lite

WorkPlace Lite is an access mode for the SMA appliance that bypasses all Access and EPC Agents and logs the user in to WorkPlace. The only prerequisite for logging into a WorkPlace Lite-enabled WorkPlace site is a modern web browser that supports HTML. Web only access is more commonly referred to as Reverse Proxy access.

The AMC administrator can:

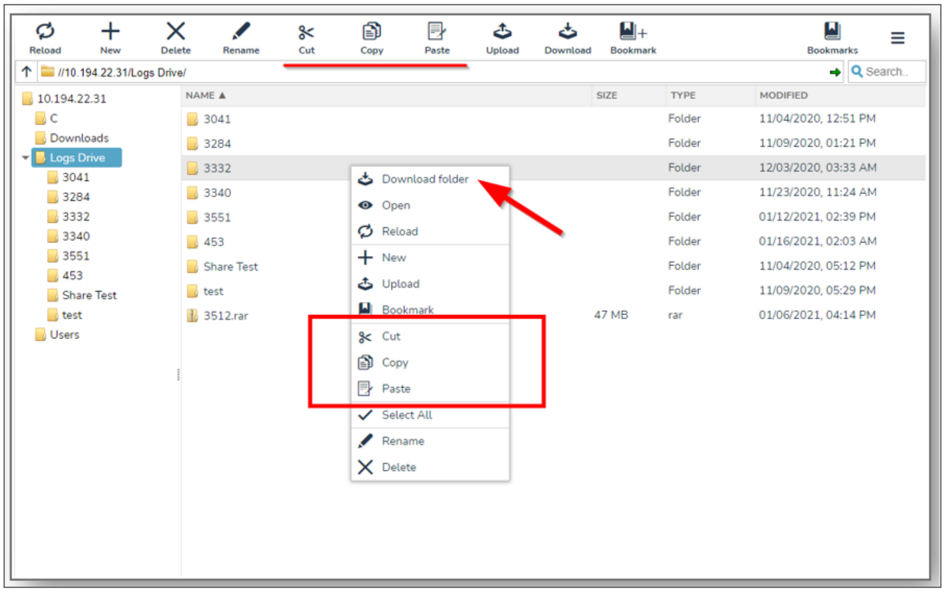
- Grant the user access to WorkPlace Lite
- Force the user to use WorkPlace Lite only
- Disable the user from accessing WorkPlace Lite

Users can select a checkbox or go to a specific WorkPlace site for Lite access. If the user checks WorkPlace Lite mode, then the system allows access to browser based graphical and text-terminal shortcuts as well as Web URL and HTML file share shortcuts. The Persistent Cookie option allows (or disallows) seamless access to SharePoint documents.

WorkPlace Enhancements

Following are the enhancements implemented in the WorkPlace.

- For enhanced user experience, following are the File Explorer improvements implemented in the current release.
    - Folder can be downloaded as a zip file.
    - You can perform the following actions on file, folder, and search results.
        - Cut
        - Copy
        - Paste



NAME ▲	SIZE	TYPE	MODIFIED
3041		Folder	11/04/2020, 12:51 PM
3284		Folder	11/09/2020, 01:21 PM
3332		Folder	12/03/2020, 03:33 AM
3340		Folder	11/23/2020, 11:24 AM
3551		Folder	01/12/2021, 02:39 PM
453		Folder	01/16/2021, 02:03 AM
Share Test		Folder	11/04/2020, 05:12 PM
test		Folder	11/09/2020, 05:29 PM
3512.rar	47 MB	rar	01/06/2021, 04:14 PM

  - When there are more than one notifications queued, the corresponding count is displayed.
  - You can sort the order of columns.
  - You can re-size column width.
  - While uploading a file on the browser, a notification pop-up is displayed, with the file upload progress. This will also prevent accidental navigation out of the browser while the file is still being uploaded.
  - Reload icon on URL bar.
  - Username on hamburger menu is displayed.
  - When navigating to parent directory, the directory tree is preserved.
- Minimal support for Internet Explorer browser.

  Since Microsoft is ending the support for Internet Explorer and for security reasons, using WorkPlace in Internet Explorer browser is not recommended.
- ActiveX is no longer supported.

  Prior to 12.4.1, ActiveX is used for IE 11, and URL launch is used for other browsers. From 12.4.1 onwards, EPC and agents are provisioned using URL scheme on all browsers to have a consistent provisioning and for better user experience across browsers.
- Audio and Video recording for RDP shortcuts and bookmarks is supported.

  For more information on how to configure audio and video recording for RDP shortcuts and bookmarks, refer to the *WorkPlace User Guide*.
- Legacy Connect Tunnel is deprecated from 12.4.1 version.

  For more information on deprecation of legacy client, refer to the *Connect Tunnel User Guide*.

Connect and OnDemand Tunnel Clients

Tunnel clients provide network-level access to all resources, effectively making each user device a virtual node on your network.

- The Connect Tunnel client provides full network and application access from a client for computers running a Windows, macOS, or Linux operating system using SMS or similar technology. The client can be provisioned either transparently using a link from the WorkPlace portal or through an executable installation package. The Connect Tunnel client provides split-tunneling control, granular access controls, and automatic proxy detection and authentication.

  ⓘ **NOTE:** The Legacy Connect Tunnel and Connect Tunnel Service (CTS) are deprecated in 12.4.1 version. For more details, refer to *SMA Connect Tunnel User Guide*.

- The OnDemand Tunnel agent provides the same features as the Connect Tunnel. Domain logins are now supported with Connect Tunnel using windows network logon. OnDemand can operate in either split-tunnel mode or redirect all traffic mode.

Mobile Connect Clients

SonicWall Secure Mobile Access Connect Tunnel with Smart Tunneling is a client component of the Secure Mobile Access Virtual private network (VPN) solution, which enables secure, authorized access to Web-based and client/server applications, and file shares.

The Mobile Connect client provides full network and application access from computers running macOS, or IOS, Android, and Chrome OS. The client is provisioned from the appropriate App store. The Mobile Connect client provides split-tunneling control, granular access controls, and automatic proxy detection and authentication.

End Point Control (EPC)

EPC components ensure that your network is not compromised when accessed from PCs in untrusted environments by enabling you to interrogate devices to determine whether they are running the programs you require. **Advanced EPC** simplifies granular end point protection by allowing you to set up device profiles using a comprehensive predefined checklist that includes security solutions from leading vendors like OPSWAT, Kaspersky, McAfee, Computer Associates, and Sophos.

Related Documentation

Refer to these SonicWall SMA documents for specific details about the various features and products of SMA 12.4:

- *Secure Mobile Access 12.4 Central Management Server Administration Guide*
- *Secure Mobile Access 12.4 WorkPlace User Guide*
- *Secure Mobile Access 12.4 Upgrade Guide*
- *Secure Mobile Access 12.4 Deployment Planning Guide*

- *Secure Mobile Access 12.4 Connect Tunnel User Guide*
- *Secure Mobile Access 12.4 8200v Getting Started Guide*

System Requirements

This section describes the system requirements for the client and administrator (server) components for Secure Mobile Access.

ⓘ **NOTE:** For additional and updated information about the system requirements and limitations of SMA 12.4.3, see the Secure Mobile Access 12.4.3 Release Notes.

Support status is indicated by the font type for items listed in the tables:

- Fully supported (normal font)
- ***Compatible with, moving into support, issues addressed as needed (bold italics)***
- *Compatible with, moving out of support (italics)*

There are no known issues with “compatible with” configurations, but they have not been specifically tested in the current release. Therefore, SonicWall does not guarantee that significant issues will not occur, and there is no guarantee of support for such issues.

Topics:

- Client Components
- Server Components

Client Components

The system requirements for client components are listed in the following tables:

- WorkPlace Lite Access
- Web-Based Clients
- Tunnel Clients
- Proxy Clients
- End Point Control

WorkPlace Lite Access

WorkPlace Lite Requirements

Operating system	Browser	Notes

• Windows 11 • Windows 10 • Version 22H2 • Version 21H2	• Edge • Chrome • Firefox • Safari	x64 and arm64
• iPhone/iPad OS • v16.x • v15.x • v14.x	• Safari	
• Android 14.x • Android 13.x • Android 12.x	• Chrome • Firefox	
• ChromeOS	• Version 103 and higher	
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	
• Linux Kernel level 4.x or later	• Firefox • Chrome	
Supported HTML bookmarks: • RDP • Telnet • SSH • VNC • Citrix (through Storefront) • Network Explorer		

Web-Based Clients

WorkPlace Portal, Translated Web, Network Explorer, Host/Port Mapping URL Access

Web-based Client System Requirements

Operating system	Browser	Notes

• Windows 11 • Windows 10	• Edge • Chrome • Firefox • Safari	
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	
• iOS • Version 16.X • Version 15.X • Version 14.X	• Safari	
• Linux Kernel level 4.x or later	• Firefox • Chrome	
• Android • Version 14.X • Version 13.X • Version 12.X	• Chrome • Firefox	

Web Application Services

Translated/Custom Port Mapped/Custom FQDN Mapped Web Application Service Requirements

Operating system	Browser	Notes
• Outlook on the Web (Exchange 2016) aka OWA	• Edge • Firefox • Chrome	
• Outlook Web Access 2013	• Edge • Firefox • Chrome	
• SharePoint 2022	• IE (32 bit and 64 bit) • Edge • Firefox • Chrome	

• SharePoint 2019	• IE (32 bit and 64 bit) • Edge • Firefox • Chrome	
• SharePoint 2016	• IE (32 bit and 64 bit) • Edge • Firefox • Chrome	
• SharePoint 2013 SP1	• IE (32 bit and 64 bit) • Edge • Firefox • Chrome	

Web Application: Generic (Simple)

Browser: Internet Explorer, Edge, Firefox, and Chrome

ⓘ **NOTE:** Support of a given web application using alias-based translation is based on the compatibility and complexity of these underlying web application. Some web applications do not work with alias-based translation, in which case custom host or port mapping URL access should be used. SonicWall only supports and tests the specifically listed applications in this section for alias-based translation access. Supports NTLM, BASIC, and forms-based Single Sign-On (SSO).

Custom Port Mapped/Custom FQDN Mapped Web Application Service Requirements

Operating system	Browser	Notes
• Domino Web Access 9.x	• Edge • Firefox • Chrome	

Web Application: Generic (Advanced)

Browser: Chrome, Edge, Firefox, and Safari.

ⓘ **NOTE:** Recommended for advanced web applications that may use, JavaScript, or other advanced web technologies. Supports NTLM, BASIC, and forms-based Single Sign-On (SSO).

Tunnel Clients

Connect Tunnel Client Requirements

Operating system	Notes
• Windows 11 • Windows 10	.NET 4.8 version

• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	
• Linux Kernel level 4.x or later	x86, x64 and arm64

OnDemand Tunnel Agent Requirements

Operating system	Browser	Notes
• Windows 11 • Windows 10	• Edge • Chrome • Firefox	
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	

Proxy Clients

OnDemand Proxy Agent Requirements (mapped Mode)

Operating system	Browser	Notes
• Windows 11 • Windows 10	• Edge • Chrome • Firefox	• Custom URL
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	• Custom URL

End Point Control

Connect Tunnel

Operating system	Browser	Notes
• Windows 11 • Windows 10	• Edge • Chrome • Firefox	• Custom URL

• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	• Custom URL
• Linux Kernel level 4.x or later		

End Point Control (Interrogator And Installer) Client System Requirements

Operating system	Browser	Notes
• Windows 11 • Windows 10	• Edge • Chrome • Firefox	• Custom URL
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	• Custom URL
• Linux Kernel level 4.x or later		

Third Party Component OESIS Requirements

Operating system	Browser
• Windows 11 • Windows 10	• Edge 113.0 or later • Chrome 113.0 or later • Firefox 113.0 or later
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari 16.0 or later
Linux Kernel level 4.x or later	

Server Components

The system requirements for the administrator components and authentication servers are listed in these tables.

- System Administration
- Authentication Servers
- ActiveSync Clients
- ActiveSync Servers

- Outlook Anywhere
- Citrix Server Farms
- Server Farms
- Graphical Terminal agents
- SMA 8200v and CMS Platforms
- API Support

System Administration

System Requirements For Management Computer Accessing AMC

Operating system	Browser	Notes
Appliance Management Console (AMC)		
• Windows 11 • Windows 10	• Edge • Chrome • Firefox	
• macOS 14.X • macOS 13.X • macOS 12.X • macOS 11.X	• Safari • Chrome	

Authentication Servers

Requirements

Operating system	Version	Notes
Microsoft Active Directory		
• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Outlook Anywhere		
LDAP servers		
• LDAP v3 compatible Servers		LDAP password change supported on IDS
• IBM Tivoli Directory Server Enterprise Edition	• v6.x	LDAP password change supported on IDS

• Oracle Directory Server Enterprise Edition	• v11g	Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1)
• NetIQ Novell eDirectory	• Directory and Resource Administrator 9	
RADIUS Protocol		
• RSA Authentication Manager	• v8.5	
• General	• Will support IP address assignment	
• Quest Defender	• v5.8.2	
Cisco Duo		
• Cloud Based Authentication	• In windows and mac CT client and Work place support 12.4.3 onwards	Duo security account and duo apps installed on mobile (Android and IOS)
SAML Authentication Servers		
• Office 365 / Azure AD		
• Google Suite/Apps/Email		
• Onelogin.com		
• Okta		

ActiveSync Clients

Requirements

Servers	Version
• Android Phone/Tablet	• Android 14.x • Android 13.x • Android 12.x
• iPhone/iPad	• v16.x • v15.x • v14.x

ActiveSync Servers

Requirements

Servers	Version
• Microsoft Exchange	• Exchange 2012 • Exchange 2019 • Exchange 2016 • Exchange 2013 SP1

Outlook Anywhere

Outlook Anywhere Using MAPI Over HTTP

Servers	Version	Clients
• Microsoft Exchange	• Exchange 2022 • Exchange 2019 • Exchange 2016 • Exchange 2013 SP1	• Outlook 2019 • Outlook 2016 • Outlook 2013

Outlook Anywhere Using RPC Over HTTP

Servers	Version	Clients
• Microsoft Exchange	• Exchange 2022 • Exchange 2019 • Exchange 2016 • Exchange 2013 SP1	• Outlook 2019 • Outlook 2016 • Outlook 2013

Citrix Server Farms

Requirements

Servers	Version
• Citrix	• Citrix XenApp 7.7 • Citrix XenDesktop v7.7

Server Farms

Requirements

Servers	Version
• VMware Horizon Server Farms	• 6.X

Graphical Terminal agents

The Secure Mobile Access appliance integrates with several popular third party agents. In some cases, the files necessary for integration are already on the appliance, and in other cases they must be copied to the appliance.

Requirements

Description	Version	Notes
Terminal Services agent • Windows 11 • Windows 10 • macOS v14.x • macOS v13.x • macOS v12.x • macOS v11.x	• Windows pre-installed MS RDP client • Microsoft Remote Desktop v8.x	
Citrix Workspace App (Receiver) • Windows 11 • Windows 10 • macOS v14.x • macOS v13.x • macOS v12.x • macOS v11.x	• Citrix Workspace App v19.x, • Citrix Receiver v4.x	
VMware View • Windows 11 • Windows 10 • macOS v14.x • macOS v13.x • macOS v12.x • macOS v11.x	• v5.x	

SMA 8200v and CMS Platforms

Component Web-based	Version

• VMWare	• ESXi • Version 8.x • Version 7.x • Version 6.x
• Microsoft Hyper-V	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016
• Amazon Web Services (AWS) Cloud	• EC2
• Azure Cloud	
• KVM	

API Support

RESTful APIs:

- Management API
- Authentication API

Capacity matrix

Capacity matrix allows you to view the total maximum capacity limits of various connections, interfaces, portals, domains, groups, users, and so on, available for SMA 1000 appliance model.

Component	Capacity limit
Max Realm Count	200
Max Number of Communities per Realm	50
Max Access Control Rules Count	1000
Max Number of Resources	5000
Max Number of Resource Groups	1000
Max Number of Resources per Resource Group	1000
Max Local Group Count	10000
Max Local User Count	50000
Max Number of Local Users per Local Group	10000
Max Workplace Site Count	200
Max Number of Workplace Styles	200
Max Workplace Layouts Count	200
Max Number of Workplace Shortcuts	2000
Max Number of Workplace Shortcut Groups	1000

Component	Capacity limit
Max Number of Workplace Shortcuts in a Group	200
Max EPC Device Zone Count	100
Max EPC Device Zone per Community Count	50
Max EPC Deny Zone Count	100
Max EPC Deny Zone per Community Count	50
Max EPC Quarantine Zone Count	100
Max EPC Device Profile Count	200
Max EPC Device Profile per Zone Count	50
Max Authentication Server Count	200
Max Number of Custom DNS Entries for Domains/kdc's	100
Max Number of Mapped Admin Users and Groups	200
Max Number of Admin Roles	50
Max Self-Signed Certificate Count	200
Max Number of Certificate Signing Requests	200
Max Number of Trusted CA Certificates	1000
Number of Static Routes Count	200
Max Number of Custom Connections	50
Max Number of Tunnel Web Resources (Custom Scan List)	100
Max EPC Device Attributes per Device Profile	100
Max Number of SNMP Hosts	200
Max Number of SNMP Trap Receivers	200
Max Number of Resource Variables	200
Max Number of Web Application Profiles	200
Max Number of Mapped Users & Groups	20000
Max Number of Dynamic Groups	1000
Max Number of Sources per Access Rule	100
Max Number of Destinations per Access Rule	100
Max Number of Links per Quarantine Zone	50
Max Number of API Keys per Administrator account	10
Max Number of Certificate groups	100
Max number of exclusions	100
Max Values in one exclusion	500

2

Installation

Installation and Initial Setup

Network Architecture

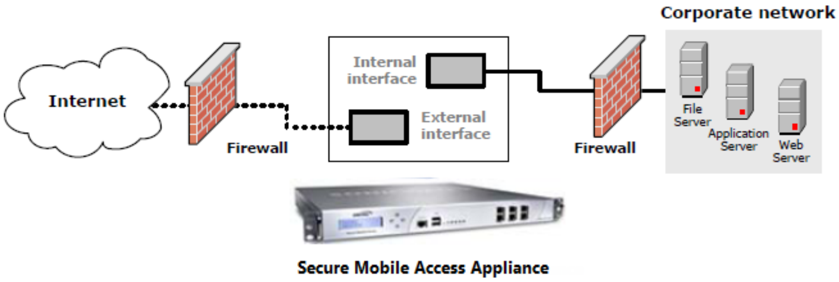
This section shows where the appliance fits into your network environment, provides installation and cabling instructions, and explains how to use the Web-based Setup Wizard (or alternatively use the command-line Setup Tool) to perform basic network configuration.

All SonicWall SMA appliances can be set up in either a dual interface or single interface configuration:

ⓘ **NOTE:** The SMA 8200v, 7200, 7210 and SMA 6200, 6210 appliances include network interfaces that can be set up to use an external load balancer.

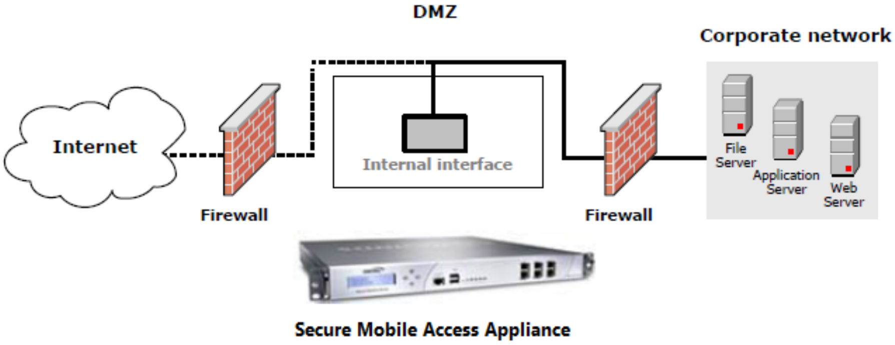
- Dual-homed Configuration (Internal and External Interfaces – see Dual-homed interface configuration) — One network interface is used for external traffic (that is, to and from the Internet), and the other interface is used for internal traffic (to and from your corporate network).

Dual-homed Interface Configuration



- Single-homed interface configuration (internal interface – see Single-Single-homed interface configuration) — A single network interface is used for both internal and external traffic. The appliance is usually installed in the demilitarized zone (or DMZ, also known as a perimeter network).

Single-homed Interface Configuration



In both configurations, incoming requests to the Secure Mobile Access services—including HTTP/S traffic for the Web proxy service—are sent over port 80 (HTTP) and port 443 (HTTPS). Traffic from the OnDemand agent is always sent over port 443. Because most networks are configured to enable traffic over these ports, you shouldn’t need to reconfigure firewalls on your network.

You should install the appliance in a location where it can connect to resources on your network, including:

- Application servers and file servers, including Web or Windows servers, and client/server applications.
- External authentication repositories (such as an LDAP, Microsoft Active Directory, or RADIUS server).
- One or more Domain Name System (DNS) servers.
- Optionally, a Windows Internet Name Service (WINS) server. This is required for browsing Windows networks using WorkPlace.

△ **CAUTION: The SonicWall SMA appliance does not provide full firewall capabilities and should be secured behind a firewall. Running without a firewall makes the appliance vulnerable to attacks that can compromise security and degrade performance.**

Although not required, enabling the appliance to communicate with these additional resources provides greater functionality and ease of use:

- Network Time Protocol (NTP) server for synchronizing the time on the appliance.
- External server for storing syslog output.

For enhanced security, you can use the integrated Let's Encrypt support to configure a free certificate. See Let's Encrypt

Preparing for the Installation

Before beginning the installation, you need to gather information about your networking environment and verify that your firewalls are properly configured to permit traffic to and from the appliance.

Topics:

- Gathering Information
- Verifying Your Firewall Policies

Gathering Information

Before configuring the appliance, you need to gather the following information. You are prompted for some of this information when running Setup Wizard (see Web-Based Configuration Using Setup Wizard) or Setup Tool (see Configuring a New Appliance Using Setup Tool), but most of it will be used when you configure the appliance in AMC (see Network and Authentication Configuration).

Information needed	Description
Settings Required to Start the Appliance Management Console	• The root password for administering the appliance • The name for the appliance (because this name is used only in log files, you don’t need to add it to DNS) • The internal IP address and, optionally, an external IP address • Select a routing mode and supply IP addresses for the network gateways to the Internet, and your corporate network

Verifying Your Firewall Policies

For the appliance to function correctly, you must open ports on your external (Internet-facing) and internal firewalls.

Topics:

- External Firewall
- Internal Firewall

External Firewall

For secure access to the appliance from a Web browser or OnDemand, you must make sure that ports 80 and 443 are open on firewalls at your site; refer to below table.

Traffic Types And Ports Used By SMA On External Network

Traffic type	Port/protocol	Usage	Required?
HTTPS	443/tcp	Encrypted network access	Y
ESP	4500/UDP	Enable ESP encapsulation of tunnel network traffic	

Internal Firewall

If you have a firewall on the internal network, you may need to adjust its policy to open ports for back-end applications with which the appliance must communicate. In addition to opening ports for standard network services such as DNS and email, you may need to modify your firewall policy before the appliance can access the services shown in the below table. Opening your firewall to permit SSH access is optional,but can be useful for performing administrative tasks from a remote system.

Traffic Types And Ports Used By SMA On Internal Network

Traffic type	Port/protocol	Usage
Microsoft networking	• 138/tcp and 138/udp • 137/tcp and 137/udp • 139/udp • 162/snmp • 445/smb	Used by WorkPlace to perform WINS name resolution, browse requests, and access file shares
LDAP (unencrypted)	389/tcp	Communicate with an LDAP directory or Microsoft Active Directory
LDAP over SSL (encrypted)	636/tcp	Communicate with an LDAP directory or Microsoft Active Directory over SSL
RADIUS	1645/udp or 1812/udp	Communicate with a RADIUS authentication server
NTP	123/udp	Synchronize the appliance clock with an NTP server
Syslog	514/tcp	Send system log information to a syslog server
SNMP	161/udp	Monitor the appliance from an SNMP management tool
Kerberos	88/tcp/udp	Authenticates service requests between two or more trusted hosts across an untrusted network

Global catalog LDAP over SSL	3269/tcp	Searches object in an Active Directory domain tree, given one or more attributes of the target object.
Global catalog LDAP	3268/tcp	LDAP service which contains data from Active Directory forests.

Installation and Deployment Process

This section outlines the process of installing, configuring, and testing the appliance, and then deploying it in a production environment. See the below table for an overview.

Installation Steps

Installation step	Description
Make a note of your appliance serial number and authentication code	You will need this information when you register your product on MySonicWall. The serial number and authentication code are printed on your appliance label; they are also displayed on the **General Settings** page in AMC.
Rack-mount the appliance and connect the cables	See Specifications and Rack Installation and Connecting the Appliance.
Turn on the appliance and begin configuration	To connect to your appliance on your internal network you must specify an internal IP address, the subnet mask, and indicate whether your appliance is part of a cluster. Use the controls on the front of the appliance. See Powering Up and Configuring Basic Network Settings.
Run Setup Wizard	The wizard guides you through the process of initial setup for your SMA appliance. See Web-Based Configuration Using Setup Wizard.
Register your appliance on MySonicWall	Register your appliance on MySonicWall. Product registration gives you access to essential resources, such as your license file and updates. To register, you need both the serial number for your appliance and its authentication code.

The SMA appliance uses a few different types of licenses. All license files must be retrieved from MySonicWall and imported to the appliance. See Software Licenses.

If you choose the Free Evaluation license on MySonicWall, you get 24/7 support for 30 days.

If you install the CMS virtual machine and do not register it with MySonicWall, you get these licenses:

- 15 Central user licenses for 3 days
- 3 managed appliances for 3 days

Both the Setup Wizard and AMC are Web-based applications for configuring the appliance. PCs running these applications must have JavaScript enabled.

Topics:

Specifications and Rack Installation

After you've unpacked the appliance, you're ready to install and configure it on your network. The appliances are designed to fit on a standard, 19-inch telecom rack. Before connecting the appliance, make sure that you have sufficient space and adequate power.

The SMA 7200,7210 and SMA 6200, 6210 include:

- Rails (in kit, not attached)
- Standard IEC 60320 C13 to NEMA 15 USA only power cord(s)
- 6 1Gb Ethernet ports
- 2 10Gb SFP+ ports (on SMA 7200, 7210)
- 2 USB ports
- 1 DIAG port
- 2 500 GB SATA hard drives:

Specifications

	SMA 7200, 7210	**SMA 6200, 6210**
Regulatory Model/Type	1RK30-0AF	1RK31-0B0
CPU	E3-1275 3.5GHz	I5-4570S 2.9GHz
RAM	4 x 16GB DDR3 1600MHz ECC	4 x 8GB DDR3 1600MHz ECC
Network ports	8 (6-port 1GE + 2-port 10Gb SFP+)	6 (6-port 1GE)
Power supply	Dual hot swappable	Fixed
Front panel illustration	See SMA 6200/6210/7200/7210 Front Panels	See SMA 6200/6210/7200/7210 Front Panels

Front Panel Controls and Indicators

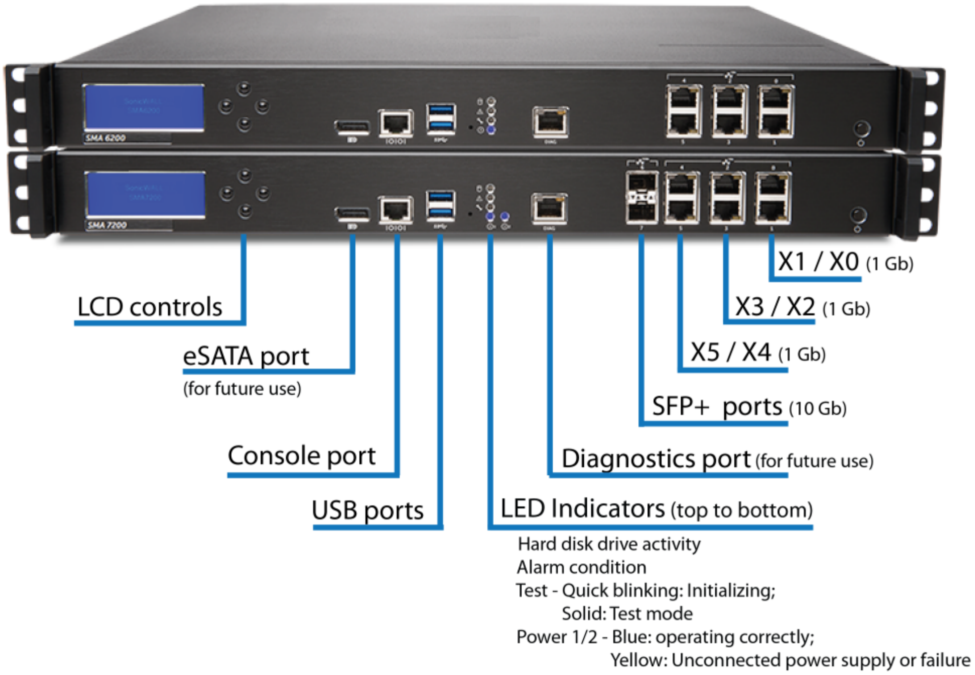
Before powering up the appliance, you should familiarize yourself with the front panel controls:

- SMA 6200/6210/7200/7210 Front Panels
- LCD Controls for the SMA 7200,7210 and SMA 6200,6210

SMA 6200/6210/7200/7210 Front Panels

The power button is at the bottom, right corner of the front panel.

Front Panels Of The SMA 6200,6210 And SMA 7200,7210



Controls And Indicators On The Front Panels

Item	Description
Hard Drive modules	Dual hard drives.

LCD display screen and controls	Displays status and configuration about the appliance. Keypad buttons are used to display appliance status and configure initial settings: • For more information on displaying appliance status and using the keypad to shut down or reboot the appliance, see LCD Controls for the SMA 7200,7210 and SMA 6200,6210. • For information on using the LCD controls during initial configuration (so that you can run Setup Wizard), see Configuring Basic Network Settings using the LCD Controls.
Console port	Connects the appliance to a personal computer with an Ethernet cable.
USB ports	There are two USB ports.
LED indicators	From top to bottom, the LED indicators are: • Hard disk drive activity • Alarm • Test • Power 1 and 2: • Blue: Operating correctly • Yellow: Unconnected power supply or failure
DIAG port	Diagnostics port.
X0: Internal network	Connects the appliance to your internal network.
X1: External network	Connects the appliance to your external network.
X2: Cluster interface	In SMA 12, the X2 interface is no longer supported for clustering. See Deprecated Features.
X3-X5	Not used.
X6 SFP+: Internal network	Connects the appliance to your internal 10Gb network.
X7 SFP+: External network	Connects the appliance to your external 10Gb network.

LCD Controls for the SMA 7200,7210 and SMA 6200,6210

Use the four-button keypad to the right of the LCD display on the SMA 6200,6210 and 7200,7210 appliances to:

- Display status and configuration information about the appliance.
- Shut down or reboot the appliance.

⚠ **CAUTION: SMA 6200,6210 and SMA 7200,7210 appliances: Remove any USB devices from the appliance before you reboot it. If a USB device is plugged in to your appliance when it is rebooted, the appliance tries to use it as a boot device. As a result, the boot information stored in the BIOS on the appliance is overwritten, and the device becomes unusable.**

LCD KEYPAD FUNCTIONS

Keypad Function	Description

Left button	Press the **Left** button once to reboot the appliance. This prompt is displayed:
	`Restart appliance?`
	`<Yes No>`
	Press the **Left** button again to reboot the appliance, or press the **Right** button to cancel the reboot.

Up button	Press the **Up** button once to display the configuration of the appliance's network settings. Each time you press it, the display shows another network setting: • Internal address • External address • Default gateway • Host name • Domain name • IP address • Netmask

Right button	Press the **Right** button once to shut down the appliance. This prompt is displayed:
	`Shut down now?`
	`<Yes No>`
	Press the **Left** button again to shut down the appliance, or press the **Right** button to cancel the shutdown.

Down button	To return to the default view at any time, or to refresh the display, press the **Down** button once.

Connecting the Appliance

Follow the appropriate instructions for your appliance model to connect the appliance to your network:

- Connecting the SMA 6200,6210 or SMA 7200,7210 Appliance
- Powering Up and Configuring Basic Network Settings

Connecting the SMA 6200,6210 or SMA 7200,7210 Appliance

For a diagram of the appliances, see SMA 6200/6210/7200/7210 Front Panels.

To connect the SMA 6200,6210 appliance:

1. Connect a network cable from your internal network to the internal interface on the appliance.
2. Optionally, connect a cable from your external network to the external interface on the appliance.

3. Connect the supplied power cord(s) to the appliance power supply and to an AC outlet.

To connect the SMA 7200,7210 appliance:

1. Connect a network cable from your internal network to the internal interface on the appliance. (X0 for 1GB or X6 for 10GB).
2. Optionally, connect a cable from your external network to the external interface on the appliance. (X1 for 1GB or X7 for 10GB).
3. Connect the supplied power cord(s) to the appliance power supply and to an AC outlet.

Powering Up and Configuring Basic Network Settings

After you've connected the appliance, you are ready to power up for the first time and begin the configuration process. You use a Web-based Setup Wizard to configure the settings needed to get the appliance up and running quickly, but to start the wizard you must first enter information that enables a Web browser to connect to your appliance.

After your appliance is configured, you can control its configuration and operation from AMC, the Appliance Management Console. On the LCD screen of the appliance you can also see basic information about the appliance (its name and internal address, for example) or restart it, which is useful if your appliance is not in the same area as the browser you use to run AMC.

ⓘ **NOTE:** You cannot run Setup Wizard on an appliance that has already been configured unless you first restore the appliance's factory default configuration settings. This applies whether you initially configured the appliance using Setup Wizard, or by running `setup_tool` from the command line. See Configuring the Appliance Using the Management Console

Configuring Basic Network Settings

To start Setup Wizard you must first enter information that enables a Web browser to connect to your appliance. The recommended procedure for initial setup is to use the LCD controls (to the right of the LCD screen on the front of your appliance) to enter minimal settings and then run Setup Wizard. Alternatively, you have the option of using Setup Tool on the command-line. These procedures are outlined below:

- Configuring Basic Network Settings Using the X0 Interface
- Configuring Basic Network Settings using the LCD Controls
- Configuring an Appliance Using Setup Tool on the Command Line

After your basic settings are entered you will be able to run the Web-based Setup Wizard, as described in Web-Based Configuration Using Setup Wizard.

Configuring Basic Network Settings Using the X0 Interface

You can connect your computer to the Ethernet port on your SMA appliance and use the Setup Wizard to configure your SMA appliance.

To configure basic network settings using the using the X0 Interface:

1. Configure your management computer with a static IP address on the same subnet as your internal (X0) interface. Set your computer to an IP address on the 192.168.0.0/24 subnet, such as 192.168.0.20, and set the subnet mask to 255.255.255.0 and the default gateway to 192.168.0.1.
2. Using an Ethernet cable, connect your management computer to the X0 port on the SMA appliance.
3. Access the wizard by starting a Web browser and typing: https://<IP address>:8443, where <IP address> matches the address you defined for the internal network interface. (The default X0 IP address is 192.168.0.10).
4. Follow the instructions in the Setup Wizard to enter your configuration settings. (Refer to Web-Based Configuration Using Setup Wizard for instructions on using the Setup Wizard.)

Configuring Basic Network Settings using the LCD Controls

There are four buttons to the right of the LCD screen on the front of your appliance that are used to enter the settings.

To configure basic network settings using the LCD controls:

1. Press the **Up** and **Down** controls to read the welcome screen or press **Right** to continue past it.
2. Set the IP address for your internal interface. To change the IP address that appears:
   a. Use the **Left** and **Right** buttons to position your cursor over the number you want to change.
   b. Use **Up** and **Down** to change the number.
   c. Press **Right** to continue to the next screen.
3. Enter your subnet mask:
   a. Use the four buttons to change the IP address displayed on the LCD screen.
   b. Press **Right** to continue to the next screen.
4. Review your settings and confirm them. In a few moments your settings are saved, and you will see instructions on browsing to a URL on your desktop computer. This is the URL for continuing your appliance configuration with Setup Wizard. For instance, the LCD display might read as follows:

   ```
   Please browse to: https://172.31.0.140:8443
   ```

For a description of configuring your appliance using Setup Wizard, see Web-Based Configuration Using Setup Wizard.

Configuring an Appliance Using Setup Tool on the Command Line

To set the minimum configuration items necessary for running Setup Wizard, you must use Setup Tool. Below is an overview of your steps; see Configuring a New Appliance Using Setup Tool for detailed instructions.

To configure basic network settings using the Setup Tool:

1. Use a terminal emulation program to establish a serial connection with the appliance from a laptop computer or terminal.

Set the serial connection options to 115200 baud, 8-n-1, and no handshake.

2. Turn the appliance on. The first time you start the system from a serial connection, Setup Tool automatically runs. When prompted to log in, type `root` for the username.
3. To configure the appliance, you are prompted to provide this information:
   - IP address and subnet mask for the internal interface
   - Default gateway used to access the internal interface (optional)

For a description of configuring your appliance using Setup Wizard, see Web-Based Configuration Using Setup Wizard.

Web-Based Configuration Using Setup Wizard

The Setup Wizard guides you through a series of required and optional steps for configuring the appliance. The AMC home page includes a **Setup Checklist** that indicates which items you have completed.

Running Setup Wizard requires the same system configuration as AMC (see System Requirements for details); in addition, JavaScript must be enabled in the browser.

To configure settings using the Setup Wizard:

1. **License agreement:** Read the terms of the End User License Agreement.
2. **Basic Settings:**
   - Specify the password you will use to access the AMC. Your password must be at least eight characters long, but no longer than 20 characters.
   - (Optional) Select a time zone, and then click **Change** to set the current time. You can synchronize the time with an NTP server later in the AMC. For more information, see Configuring Time Settings. It is important to ensure that the appliance’s date and time settings are correct for your time zone before you import your license file.
3. **Network Settings:**
   - Enter a name for the appliance (the default is *SMAAppliance*).

     ⓘ | **TIP:** Because this name is used only in log files, you don’t need to add it to DNS.
   - The IP address and subnet mask for the internal interface (connected to your private network) is shown. For a dual-homed configuration, enter the IP address and subnet mask for the external interface.
4. **Routing:** To leverage an existing router, select the dual gateway option to reach your resources. To restrict incoming appliance traffic to just a few routes or subnets, select the single gateway option and enter the routes or subnets as static routes later in the AMC.

   If the appliance is on a different network than the computer you will use to access AMC, you must set up routing to maintain access to AMC.
5. **Name Resolution:** The appliance must be able to perform name resolution to reach resources on your internal network. Enter a default domain, which is the domain in which the appliance is located (such as `yourcompany.com`).

6. **User access:** You can give users full network access by provisioning the OnDemand Tunnel access agent. If you do, you also need to specify the Source NAT address that appears to back-end servers as the source of client traffic. This must be an IP address that is on the same subnet as the internal interface, and is not in use elsewhere.

The end of the Setup Wizard process displays your settings. Proceed to AMC, the management console, for the last steps in the configuration process. See Configuring the Appliance Using the Management Console for details.

Configuring the Appliance Using the Management Console

The final installation and deployment settings are done in AMC.

To configure the appliance in the AMC:

1. Log in to AMC.
2. Register the appliance on MySonicWall and retrieve your license file.

   When you register your appliance, you must enter both your serial number and your authentication code, which is the hardware identifier for the appliance you purchased:

   - The serial number is printed on a label on the outside of your appliance and also available in the **Licensing** page..
   - The authentication code is displayed in AMC: click **General Settings** from the main navigation menu, and then look in the **Licensing** area.

   When you receive your SMA appliance there is a single user license on it, valid for three days. To become familiar with the AMC and test it in your environment with additional users, request a lab license. After initial setup and testing, download your license file from MySonicWall and then import it to the appliance.

   See Managing Licenses.
3. Define one or more authentication servers.

   Authentication is used to verify the identity of users. When configuring an authentication server, you are prompted to specify a directory type (LDAP, Microsoft Active Directory, RADIUS, or local users) and a credential type (username/password, token, or digital certificate).

   See Managing User Authentication.
4. Configure a server certificate.

   The appliance encrypts information using the Secure Sockets Layer (SSL) protocol. You can use Let's Encrypt certificate authority that is public, free, API-driven, and trusted by browsers/clients. You can create a selfsigned certificate using AMC for evaluation or testing purpose.

   See Certificates.
5. Define application resources and groups.

   Application resources include TCP/IP-based resources (such as client/server applications, file servers, or databases), Web-based resources (including Web applications or Web sites) that run over HTTP, and Windows network share resources (to be accessed in WorkPlace). Resource definitions can include variables, so that a single resource can, for example, derive its network name or address based on each user.

See Creating and Managing Resources.

6. Define users and groups.

   User and group definitions are used in access control rules to control access to application resources.

   See Managing Users and Groups.

7. Define realms and communities.

   Realms enable the appliance to directly integrate with authentication servers, eliminating the need to create and manage accounts for each user who needs access to your network. Communities aggregate users with similar access needs and End Point Control requirements.

   See Managing User Authentication.

8. Create access control rules.

   Access control rules determine what resources are available to users and groups.

   See Access Control Rules.

9. Configure shortcuts for WorkPlace.

   To provide your users with easy access to a Web, file system, or graphical terminal resource from within WorkPlace, you may want to create shortcuts in WorkPlace.

   See Working with WorkPlace Shortcuts.

10. (Optional) Configure the network tunnel service.

    If you plan to deploy the network tunnel clients, you must configure the network tunnel service and allocate IP address pools for the clients.

    See Configuring the Network Tunnel Service.

11. (Optional) Enable and configure End Point Control.

    End Point Control optionally deploys data protection components designed to safeguard sensitive data and ensure that your network is not compromised when accessed from PCs in untrusted environments. End Point Control is deployed through communities.

    See End Point Control and Using End Point Control Restrictions in a Community.

12. Apply your changes.

    To activate your configuration changes, you must apply them.

    See Applying Configuration Changes.

13. Test system accessibility.

    Verify that the appliance can access your external user repositories, and ensure that the resources on your network are accessible.

    See Troubleshooting.

Moving the Appliance into Production

After you have tested the appliance sufficiently in your network environment and determined how you want it to work, you’re ready to move it into its permanent home.

To move the appliance into production:

1. Reconfigure the appliance with new address information.

   If the network environment changed when you moved the appliance into production, you must reconfigure the basic network settings and adjust any of the following values if they have changed:

   - IP addresses for the internal and external interfaces
   - Default gateway IP addresses
   - Static routes
   - Default DNS domain and DNS server IP address

2. Register the appliance with DNS.

   If you haven't already registered the appliance with your company's DNS, do this now. This ensures that external users can access your network resources using a fully qualified domain name instead of an IP address. Edit your DNS server's database to include the fully qualified domain name contained in the appliance's certificate and any WorkPlace sites.

3. Obtain a free trusted certificate using Let's Encrypt., this feature is integrated into AMC.

   You may want to obtain a Let's Encrypt is a certificate authority that is public, free, API-driven, and trusted by browsers/clients.)

   For more information on generating certificates, see Let's Encrypt.

4. Adjust your firewall policies.

   If you have an Internet-facing firewall, you may need to adjust its policy to open ports required by the appliance. By default, the Web proxy service communicates using port 443/tcp (it uses port 443/tcp for HTTPS and port 80/tcp for HTTP).

   If you enable ESP encapsulation of tunnel network traffic, you'll need to open port 4500/UDP.

   ⓘ **NOTE:** ESP encapsulation is enabled by default, but the system falls back to the default SSL/TLS if ESP encapsulation cannot be brought up, as when port 4500/UDP is blocked by the firewall.

   If you have a firewall that faces the internal network, you may need to adjust the policy for that firewall to open ports for any back-end applications with which the appliance must communicate (if these ports are not already open). For instance, if you use an LDAP or Microsoft Active Directory server for authentication, you must open port 389/tcp on your internal firewall. For RADIUS, open ports 1645/ucp and 1812/udp.

   If you're using WorkPlace to access Windows network shares, you must also open internal ports on your internal firewall so that WorkPlace can perform name resolution, make browse requests, and connect to file shares.

   For more information, see Gathering Information.

5. Create shortcuts and deploy WorkPlace.

   If you use WorkPlace as an interface to Web-based resources and to provide Web-based access to Windows network share and graphical terminal resources, you must create shortcuts (seeWorking with WorkPlace Shortcuts). You should also publish the WorkPlace URLs so your users know how to access resources through your VPN.

   You may want to customize the appearance of WorkPlace for your environment. See Configuring WorkPlace General Settings for more information.

Powering Down and Restarting the Appliance

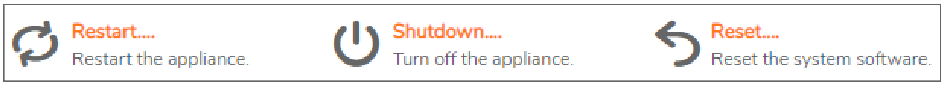
When it's time to power down or restart the appliance, be sure to follow the proper procedure. The appliance stores important data in memory while it is running. That data must be written to the hard disk before you turn off the power.

⚠ **CAUTION: Powering down the appliance improperly can result in loss of data and leave the system's files in an inconsistent state. For SMA 7200,7210 and SMA 6200,6210 appliances: Remove any USB devices from the appliance before you reboot it. If a USB device is plugged in to your appliance when it is rebooted, the appliance tries to use it as a boot device. As a result, the boot information stored in the BIOS on the appliance is overwritten, and the device becomes unusable.**

To power down or restart the appliance in AMC:

1. In the AMC, navigate to **System Configuration > Maintenance**.

   The **Maintenance** page displays.



2. Click the appropriate button:

   - To restart the appliance, click **Restart**.

     AMC stops responding. After the appliance restarts, you can log in to AMC again.

   - To shut down the appliance, click **Shutdown**.

     AMC stops responding and the appliance powers down. You do not need to press the power button on the front panel.

   All appliance models can be shut down or restarted at the appliance:

   a. On the front of the appliance, press the **Down** button on the four-button keypad to get to the main LCD menu.

   b. Scroll down until you reach the option you want, **Restart** or **Shutdown**.

   c. Both options display a confirmation message; press the **Left** button to continue.

   d. The results are the same as restarting or shutting down in AMC:

      - AMC stops responding; after the appliance restarts, you can log in to AMC again.
      - AMC stops responding and the appliance automatically powers down. You do not need to press the power button on the front panel.

Next Steps

After you have completed the initial network setup, use AMC to continue configuring the appliance. AMC is accessible using a Web browser.

ⓘ | **TIP:** If you're new to AMC, you might want to read Working with Appliance Management Console.

If you're ready to continue configuring the appliance, see Network and Authentication Configuration.

3

Management

- User Management
- Working with Appliance Management Console

Working with Appliance Management Console

Topics:

- Logging In to AMC
- Logging Out
- AMC Basics
- Administrator Accounts
- Managing Multiple Secure Mobile Access Appliances
- Working with Configuration Data
- Deleting Referenced Objects

Logging In to AMC

This section introduces the Appliance Management Console (AMC), a Web-based interface for managing the appliance.

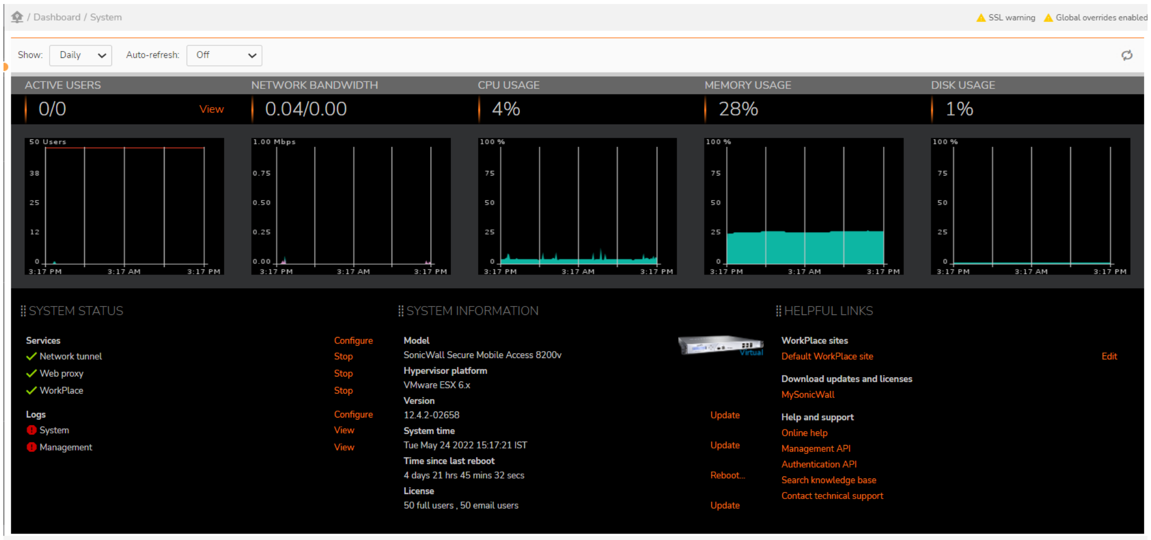
Before logging in to AMC, you need the host name or IP address you typed for the internal interface during the initial setup with Setup Tool.

To log into AMC:

1. Start your Web browser and type the URL `https://<ipaddress>:8443`, where `<ipaddress>` matches the address you specified for the internal interface when you ran Setup Tool or Setup Wizard.
2. Enter `admin` in the **Username** text field.
3. Enter the root password you created using Setup Tool in the **Password** text field.

4. Select the **Management Console** in the **Log in using** drop-down menu.
5. Click **Login**.

   The AMC home page displays.



Show: Daily
Auto-refresh: Off

ACTIVE USERS 0/0
NETWORK BANDWIDTH 0.04/0.00
CPU USAGE 4%
MEMORY USAGE 28%
DISK USAGE 1%

Services
✓ Network tunnel
✓ Web proxy
✓ WorkPlace

Logs
● System
● Management

Model
SonicWall Secure Mobile Access 8200v
Hypervisor platform
VMware ESX 6.x
Version
12.4.2-02658
System time
Tue May 24 2022 15:17:21 IST
Time since last reboot
4 days 21 hrs 45 mins 32 secs
License
50 full users , 50 email users

WorkPlace sites
Default WorkPlace site
Download updates and licenses
MySonicWall
Help and support
Online help
Management API
Authentication API
Search knowledge base
Contact technical support

6. Review the system statistics and use the functions on the right to configure and maintain your system.
7. Click the **Help** icon at the top for details about configuring your appliance.

For information on changing the AMC password, see Editing Administrator Accounts.

ⓘ **NOTE:** Avoid multiple administrators making changes to AMC simultaneously. For more information, see Avoiding Configuration Conflicts with Multiple Administrators.

Logging Out

It is important to preserve the security of your AMC administrator account. When you're finished working in AMC, click **Log out** in the upper-right portion of the screen. If you terminate a session by simply closing your Web browser, your session remains active until it times out (after 15 minutes of inactivity). There is an exception to this rule that you should be aware of; see Appliance Sessions for details.

AMC Basics

This section describes the basics of working with AMC. All configuration data is encrypted using SSL as it's transferred between AMC and your browser, ensuring that it remains secure. To increase security, AMC should be used within a trusted network (on an internal network that is behind a firewall). See Working with Certificates FAQs for more details.

Topics:

- A Quick Tour of the AMC Interface
- Adding, Editing, Copying, and Deleting Objects in AMC
- Getting Help

A Quick Tour of the AMC Interface

The AMC interface will be familiar to anyone who has worked with similar Web-based security management applications. Here are some basic notes about working with AMC.

Topics:

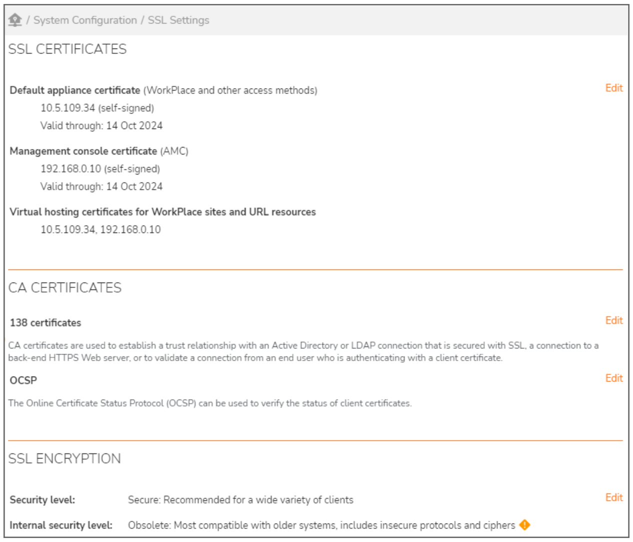
- Summary Pages
- Tables and Tabs
- Filters
- Page Links
- Editing an Object
- Changing the Page View
- Expanded View of List Details
- Required Fields and Errors
- Assigning Names and Descriptions
- Saving Changes on a Page
- AMC Status Area
- Version Number and Product Serial Number

Summary Pages

Several top-level pages in AMC are summary pages that provide quick access to subordinate configuration pages and display summaries of key configuration settings and other status information. These summary pages are:

- Agent Configuration
- General Settings
- Network Settings
- SSL Settings
- Authentication Servers
- Services

For example, the **SSL Settings** page displays which SSL certificates are being used, how many are currently installed.



/ System Configuration / SSL Settings

SSL CERTIFICATES

Default appliance certificate (WorkPlace and other access methods) Edit

10.5.109.34 (self-signed)

Valid through: 14 Oct 2024

Management console certificate (AMC)

192.168.0.10 (self-signed)

Valid through: 14 Oct 2024

Virtual hosting certificates for WorkPlace sites and URL resources

10.5.109.34, 192.168.0.10

CA CERTIFICATES

138 certificates Edit

CA certificates are used to establish a trust relationship with an Active Directory or LDAP connection that is secured with SSL, a connection to a back-end HTTPS Web server, or to validate a connection from an end user who is authenticating with a client certificate.

OCSP Edit

The Online Certificate Status Protocol (OCSP) can be used to verify the status of client certificates.

SSL ENCRYPTION

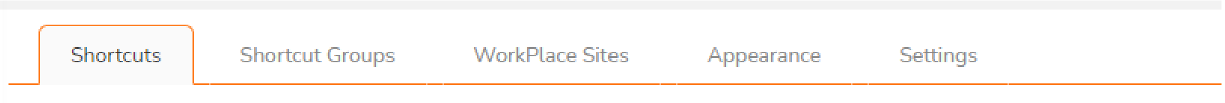
Security level: Secure: Recommended for a wide variety of clients Edit

Internal security level: Obsolete: Most compatible with older systems, includes insecure protocols and ciphers

Tables and Tabs

Many AMC pages use a tabular layout to present the objects you'll be managing. The tables include scroll bars, which make it easier for you to keep the main elements on the page (including the navigation bar, header, and footer) in view when working with long lists. You can also sort the data displayed in some tables by clicking the underlined column headings.

In some cases, you'll use tabs to switch between modes. For example, you'll use tabs to switch between managing resources, groups of resources, and variables used in defining resources.



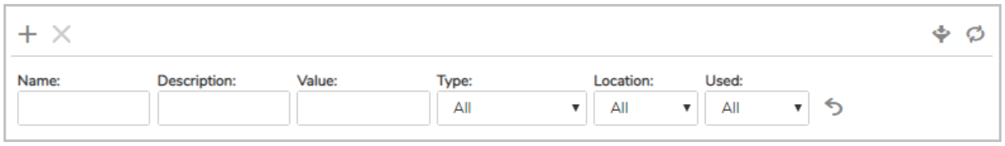
Filters

On pages in AMC that contain a list of items that can grow to many pages in a large configuration, filtering is available to make it easier for you to find what you are looking for. Filters are available on the AMC pages shown in the below table:

Pages Containing Filters

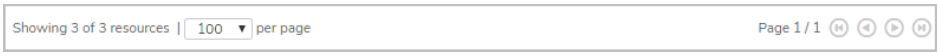
Security Administration	**User Access**
Access Control	WorkPlace
Resources	WorkPlace > Shortcut Groups
Resources > Resource Groups	**Monitoring**
Users & Groups	User Sessions
Users & Groups > Local Accounts	Logging

The exact filters vary slightly with each page, but the following functionality is consistent across all pages:



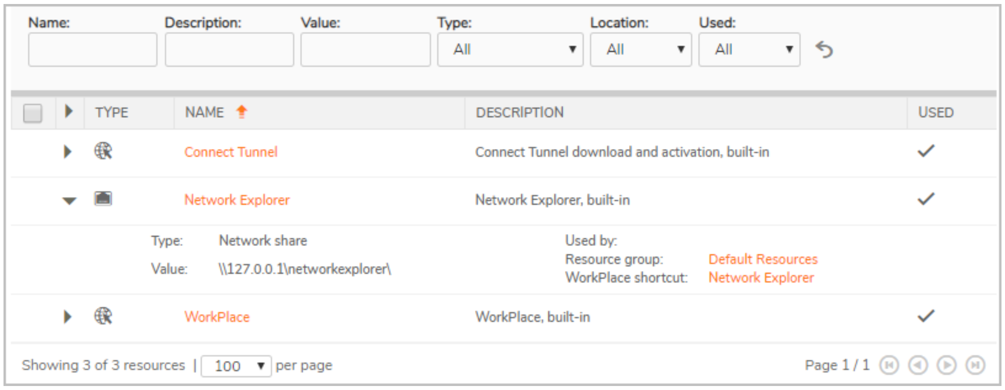
Name:	Description:	Value:	Type:	Location:	Used:
			All	All	All

- There is a **reset** link that resets the filter fields to their default values.
- There is a red **active** indicator that indicates that the page was loaded using filters, meaning that the list may not be displaying all the configured items.
- There is a **Refresh** button that reloads the page with the specified filters applied.
- The filters are stored so that the next time you load the page, it uses the same filters that were last applied. The filters are stored across sessions, so even if you log out and log back in, the same filters will be used.
- There is a footer at the bottom of the list that shows the number of items displayed and the total number of items in the list. If filtering is active, there is a (**filtered**) indicator and a **Show all** link that resets the filters to the defaults and refresh the page to display all items in the list.



Showing 3 of 3 resources | 100 per page Page 1 / 1

In general, the available filters map to the displayed columns in the list. In some cases, such as **Resource Groups** or **Shortcut Groups**, you can filter the list based on the members of the group, which is not a column in the list. As another example, on the **Resources** page you could filter the list based on something in the **Value** attribute, which is not a column, but is visible when an item in the list is expanded.



Name:	Description:	Value:	Type:	Location:	Used:
			All	All	All

TYPE	NAME	DESCRIPTION	USED
	Connect Tunnel	Connect Tunnel download and activation, built-in	✓
	Network Explorer	Network Explorer, built-in	✓
	WorkPlace	WorkPlace, built-in	✓

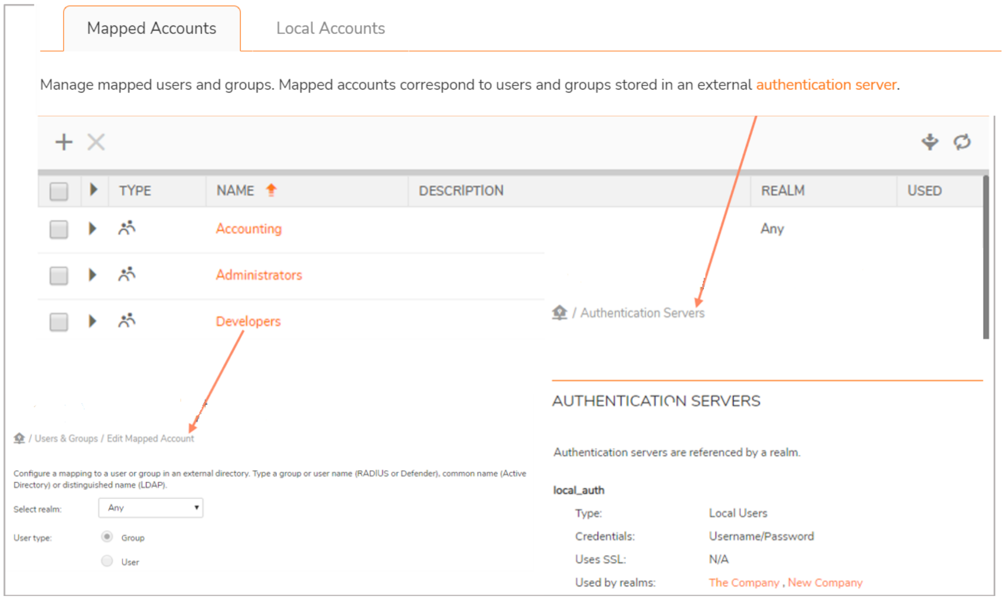
Type: Network share
Value: \\127.0.0.1\networkexplorer\
Used by:
Resource group: Default Resources
WorkPlace shortcut: Network Explorer

Showing 3 of 3 resources | 100 per page Page 1 / 1

One way that you could use this feature for custom filtering is to create your own “tags” by adding a custom string to the **Description** field of related items. For example, if a certain set of resources are all used by one department or for one customer, you could add a keyword or tag to the description of those resources, and then use the filtering capability to quickly display only the resources that contain the special keyword or tag.

Page Links

Links to other pages are shown in orange and are underlined when you hover your cursor over them. Clicking on the link displays the page.



Manage mapped users and groups. Mapped accounts correspond to users and groups stored in an external authentication server.

□	▶	TYPE	NAME	DESCRIPTION	REALM	USED
□	▶		Accounting		Any	
□	▶		Administrators			
□	▶		Developers			

/ Users & Groups / Edit Mapped Account

Configure a mapping to a user or group in an external directory. Type a group or user name (RADIUS or Defender), common name (Active Directory) or distinguished name (LDAP).

Select realm: Any

User type: ● Group ○ User

/ Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

local_auth

Type:	Local Users
Credentials:	Username/Password
Uses SSL:	N/A
Used by realms:	The Company , New Company

Editing an Object

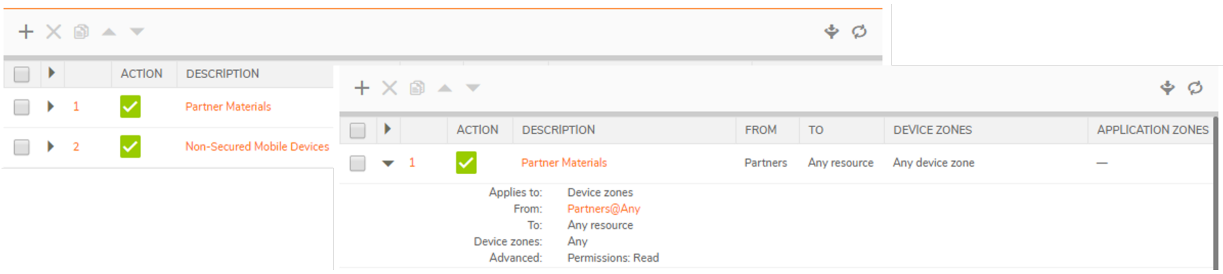
In most of the tables used to display lists of objects, the name field (or in the case of the **Access Control** page, the rule number) is hyperlinked. To edit an object, click its hyperlink.

Changing the Page View

Some of the longer, more complex pages in AMC hide the edit controls used to configure advanced features. This makes it easier for you to focus on the most important configuration options. To view hidden options, click the down arrow (click the up arrow to hide them again).

Expanded View of List Details

AMC pages that display lists of objects, such as the **Access Control** page, let you view details about an object by clicking the right arrow (▶) in the second column. To return to the one-line view, click the down arrow (▼).



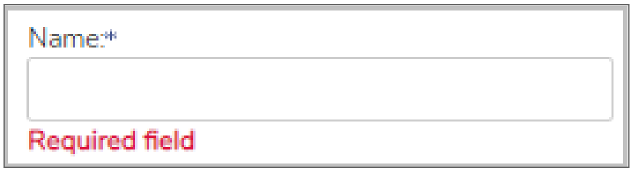
□	▶		ACTION	DESCRIPTION
□	▶	1	✓	Partner Materials
□	▶	2	✓	Non-Secured Mobile Devices

□	▶		ACTION	DESCRIPTION	FROM	TO	DEVICE ZONES	APPLICATION ZONES
□	▼	1	✓	Partner Materials	Partners	Any resource	Any device zone	—

Applies to:	Device zones
From:	Partners@Any
To:	Any resource
Device zones:	Any
Advanced:	Permissions: Read

Required Fields and Errors

Required fields are indicated in AMC with an asterisk. If you omit a value for a required field and click **Save**, a red message appears beneath the field indicating that it is required. A red message is also used to indicate an error (for example, if you type an invalid value).



Name:*

Required field

Assigning Names and Descriptions

Most of your time in AMC will be spent managing three types of objects:

- Access control rules
- Resources
- Users and groups

When you create these objects, AMC requires that you type a name. AMC also has a space for you to type an optional description.

Although not required, meaningful descriptions can help you remember critical details about the objects you're managing, such as the purpose of an access rule or what resources are in a subnet range. A good description is especially helpful when managing a group of objects; when you return to AMC later to manage a large group of network resources, for example, you'll be glad to have a description reminding you of what's in the group.

ⓘ **NOTE:** Assigning identical names to different types of objects (for example, assigned "Employee" to an authentication server, realm, and access rule), while allowed, can make troubleshooting some issues more difficult. It is recommended that you identify each object uniquely (for example, "Employee Realm").

Saving Changes on a Page

On some AMC pages you can **Save** or **Cancel** the changes you make. If you click **Cancel**, or use the **Back** button in your browser, your changes are not saved.

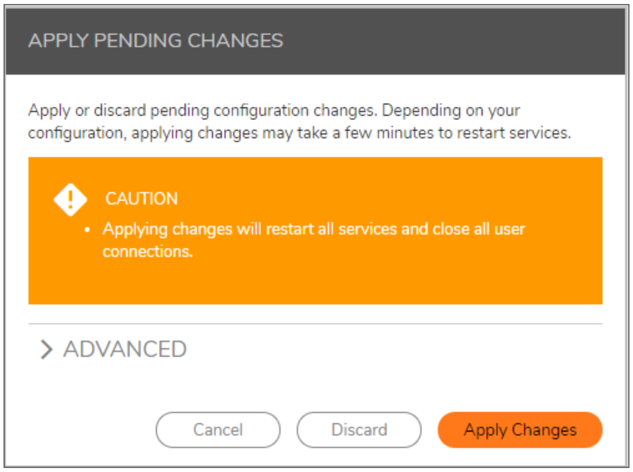
AMC Status Area

A status area just beneath the SonicWall Secure Mobile Access banner displays important information:

Secure Mobile Access | App86

Each message has an indicator for the importance of the information; for example, a yellow warning sign. Each of these messages is a link that displays either:

- A page with further information: for example, clicking on **Pending changes** displays:



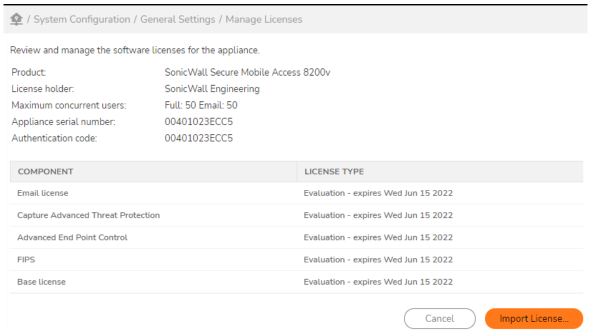
APPLY PENDING CHANGES

Apply or discard pending configuration changes. Depending on your configuration, applying changes may take a few minutes to restart services.

CAUTION

- Applying changes will restart all services and close all user connections.

- The relevant page. For example, clicking on **License expired** displays **System Configuration > General Settings > Manage Licenses**.



Review and manage the software licenses for the appliance.

Product:	SonicWall Secure Mobile Access 8200v
License holder:	SonicWall Engineering
Maximum concurrent users:	Full: 50 Email: 50
Appliance serial number:	00401023ECC5
Authentication code:	00401023ECC5

COMPONENT	LICENSE TYPE
Email license	Evaluation - expires Wed Jun 15 2022
Capture Advanced Threat Protection	Evaluation - expires Wed Jun 15 2022
Advanced End Point Control	Evaluation - expires Wed Jun 15 2022
FIPS	Evaluation - expires Wed Jun 15 2022
Base license	Evaluation - expires Wed Jun 15 2022

Version Number and Product Serial Number

The version of the current system software and the product serial number are displayed in the page footer of every page in AMC.

In addition to the version number, the **System Status** and **Maintenance** pages display a list of any hot fixes that have been applied. The version number and hot fix information is useful for planning system updates, and you need to have it when contacting SonicWall Technical Support.

Adding, Editing, Copying, and Deleting Objects in AMC

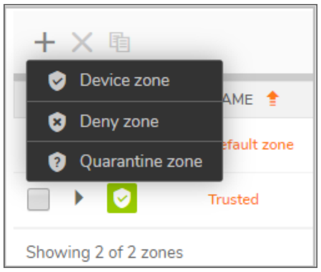
AMC features a standardized user interface for managing most objects, such as resources, access control rules, users, communities, End Point Control zones and device profiles, and other items used to organize and operate your VPN.

Following are the basic procedures for adding, editing, copying, and deleting objects in AMC, although there may be some minor variations depending on the object and AMC page you're working on. The examples provided here use the **End Point Control Zones** page.

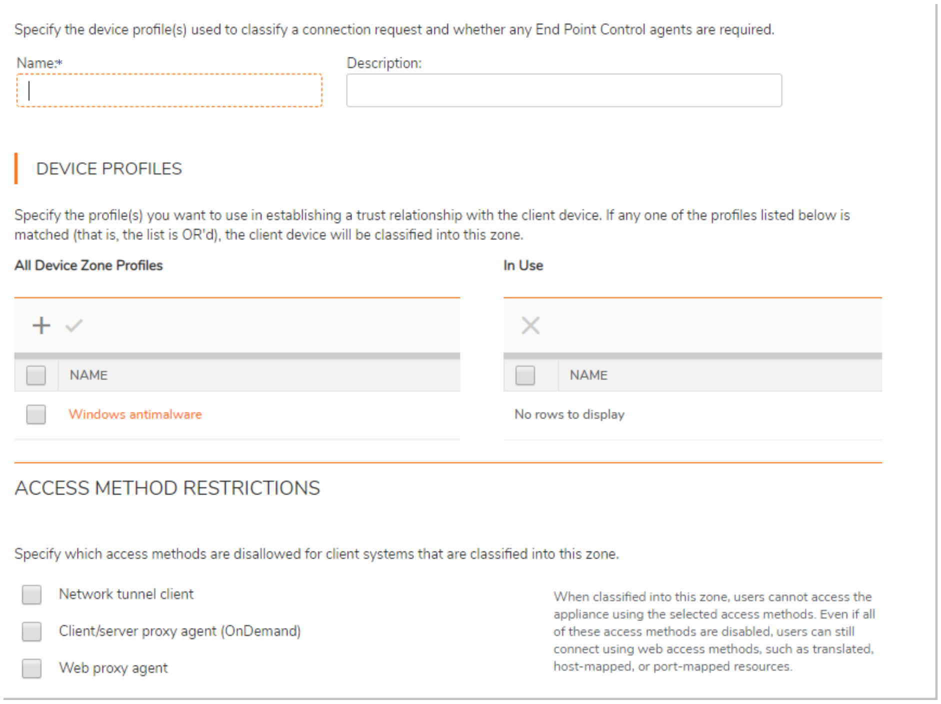
To add a new object in AMC:

1. Click the **+** (New) icon on the page listing the type of object you want to create.
2. Select the option you want to create.

   This example uses **Device zone**.



   The **Add Device Zone** page displays.



Specify the device profile(s) used to classify a connection request and whether any End Point Control agents are required.

Name:*

Description:

DEVICE PROFILES

Specify the profile(s) you want to use in establishing a trust relationship with the client device. If any one of the profiles listed below is matched (that is, the list is OR'd), the client device will be classified into this zone.

All Device Zone Profiles

□	NAME
□	Windows antimalware

In Use

□	NAME
No rows to display	

ACCESS METHOD RESTRICTIONS

Specify which access methods are disallowed for client systems that are classified into this zone.

□ Network tunnel client

□ Client/server proxy agent (OnDemand)

□ Web proxy agent

When classified into this zone, users cannot access the appliance using the selected access methods. Even if all of these access methods are disabled, users can still connect using web access methods, such as translated, host-mapped, or port-mapped resources.

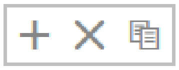
3. Complete the relevant information for the object.
4. Click **Save** at the bottom of the screen.

To edit an object in AMC:

1. On the page that lists the object you want to edit, click the link for the name (or in some cases, the number) of the object you want to modify. For a quick description of the object, an expand (+) button is available on most lists.
2. Make any changes to the information for the object.
3. Click **Save**.

To copy an object in AMC:

1. On the page that lists the object you want to copy, select the checkbox to the left of the object.
2. Click **Copy**.

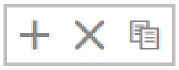


3. Make any changes to the information about the source object, and be certain to assign the object a new name.
4. Click **Save**.

To delete an object in AMC:

> ⓘ **NOTE:** You cannot delete an object that is still associated with other objects. For information, see Deleting Referenced Objects.

- On the page that lists the object you want to delete, select the checkbox to the left of the object.
- Click **Delete**.



Getting Help

Every AMC page includes a **Help** button (in the upper right portion of the page) that navigates you to the Technical Documentation site of SonicWall. By default, the latest SMA documents are displayed. In the search bar, enter the respective document or feature you are looking for and click on the Search icon to fetch the documents list. There are various filters available to enhance the search capabilities.

Administrator Accounts

This section describes:

- Managing Administrator Accounts and Roles
- Avoiding Configuration Conflicts with Multiple Administrators

Managing Administrator Accounts and Roles

AMC enables you to create multiple administrator accounts, each with a separate username and password. You can then assign roles to administrators, specifying which features in AMC they can use, and their levels of access.

By default, AMC is configured with a primary administrator role that has full access to all areas of AMC. Only the primary administrator can add, edit, or delete other administrator accounts.

ⓘ **NOTE:** If FIPS is enabled, and if the administrator password is lost, you cannot regain the administrative access to the appliance. However, assigning the administrator with the super administrator role, allows you to disable the FIPS and can recover from a lost or corrupted administrator or root password.

Topics:

- Adding Authentication Server
- Adding Administrator Accounts
- Editing Administrator Accounts
- Defining Administrator Roles
- Editing Administrator Roles

Adding Administrator Accounts

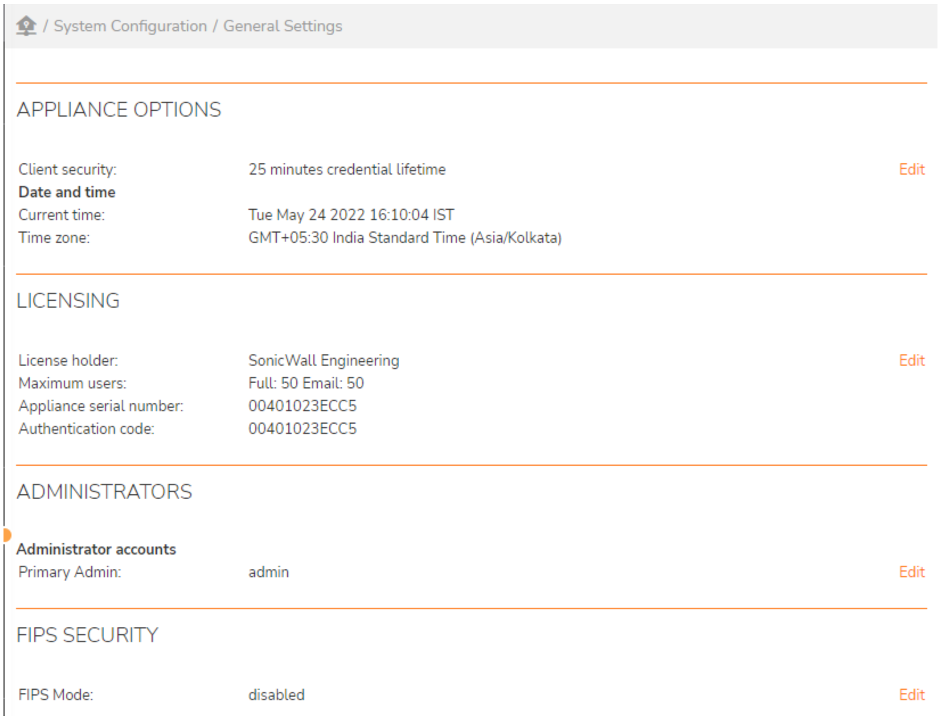
You can create additional administrator accounts if more than one person is responsible for managing policy and you want each person to have individual login credentials. Only the “primary” administrator-whose default name of *admin* cannot be changed-can create, modify, and delete secondary administrator accounts.

ⓘ **NOTE:** Before creating administrator accounts it is important to define the authentication server first to authenticate the administrator accounts. See Adding Authentication Server.

By default, the preconfigured roles include the ability to view all forms of session data and to terminate sessions. See Viewing User Sessions and Ending User Sessions for more information.

To add an administrator account:

1. In the AMC, navigate to **System Configuration > General Settings**.



/ System Configuration / General Settings

APPLIANCE OPTIONS

Client security:	25 minutes credential lifetime	Edit
Date and time		
Current time:	Tue May 24 2022 16:10:04 IST	
Time zone:	GMT+05:30 India Standard Time (Asia/Kolkata)	

LICENSING

License holder:	SonicWall Engineering	Edit
Maximum users:	Full: 50 Email: 50	
Appliance serial number:	00401023ECC5	
Authentication code:	00401023ECC5	

ADMINISTRATORS

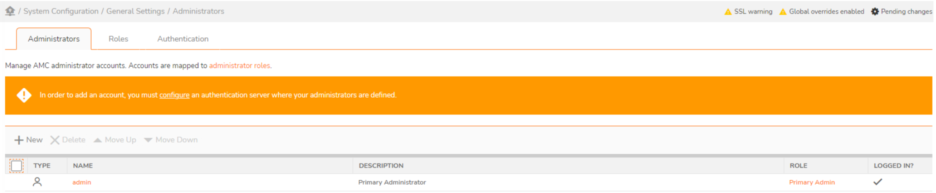
Administrator accounts		
Primary Admin:	admin	Edit

FIPS SECURITY

FIPS Mode:	disabled	Edit

2. In the **Administrator accounts** section under **Administrators**, click **Edit**.

   The **Administrators** page displays.



/ System Configuration / General Settings / Administrators

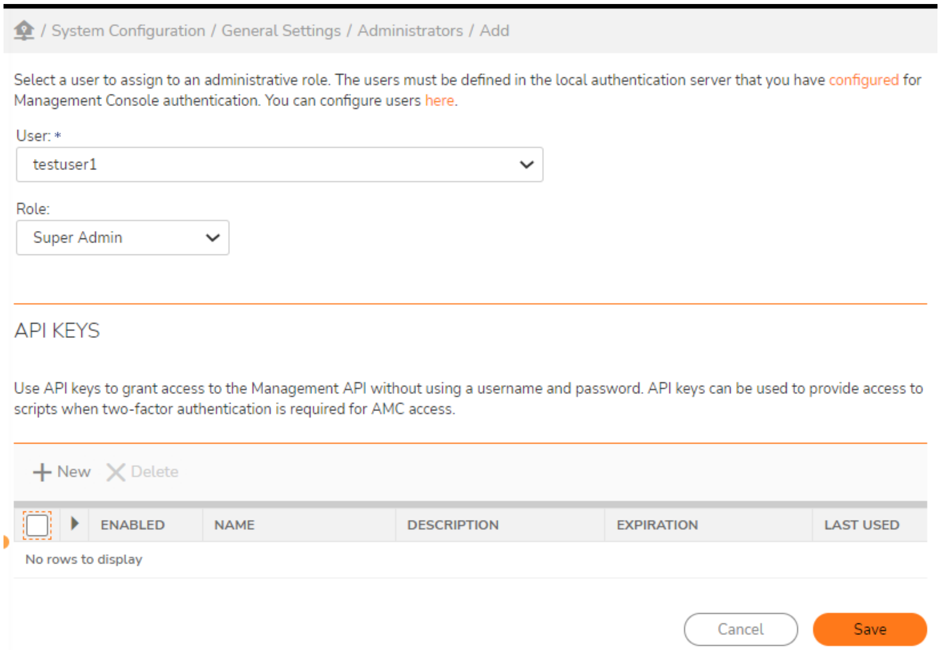
Manage AMC administrator accounts. Accounts are mapped to administrator roles.

In order to add an account, you must configure an authentication server where your administrators are defined.

□	TYPE	NAME	DESCRIPTION	ROLE	LOGGED IN?
	👤	admin	Primary Administrator	Primary Admin	✓

3. Click the **+** (New) icon.

   The **Add Administrator** page displays.



/ System Configuration / General Settings / Administrators / Add

Select a user to assign to an administrative role. The users must be defined in the local authentication server that you have configured for Management Console authentication. You can configure users here.

User: * testuser1

Role: Super Admin

API KEYS

Use API keys to grant access to the Management API without using a username and password. API keys can be used to provide access to scripts when two-factor authentication is required for AMC access.

ENABLED	NAME	DESCRIPTION	EXPIRATION	LAST USED

No rows to display

4. In the **User** drop-down menu, select a user.
5. Select an Administrator Role from the **Role** drop-down menu. AMC provides preconfigured roles, which are defined on the **Add Administrator Role** page; see Preconfigured role descriptions. You can modify these preconfigured roles, or create new roles (see Defining Administrator Roles):

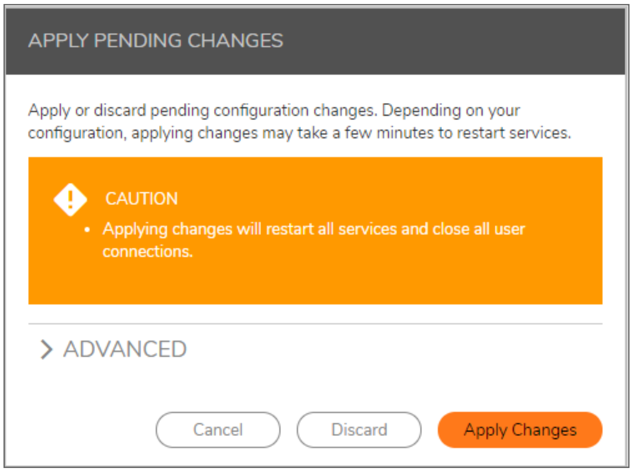
   NOTE: By default, the preconfigured roles include the ability to view all forms of session data and to terminate sessions. See Viewing User Sessions and Ending User Sessions for more information.

   Preconfigured Role Descriptions

Preconfigured role	Description
Super Admin	Has read/write access to all pages in AMC
Security Admin	Has read/write access to security administration and monitoring pages in AMC, and view access to system settings
System Admin	Has read/write access to system and monitoring pages, and view access to security pages

6. Click **Save**.
7. Click **Pending changes** at the top of the page.

   The **Apply Pending Changes** dialog displays.



APPLY PENDING CHANGES

Apply or discard pending configuration changes. Depending on your configuration, applying changes may take a few minutes to restart services.

CAUTION

- Applying changes will restart all services and close all user connections.

8. Click **Apply Changes**.

Editing Administrator Accounts

ⓘ **NOTE:** For information on deleting administrator accounts, see Adding, Editing, Copying, and Deleting Objects in AMC

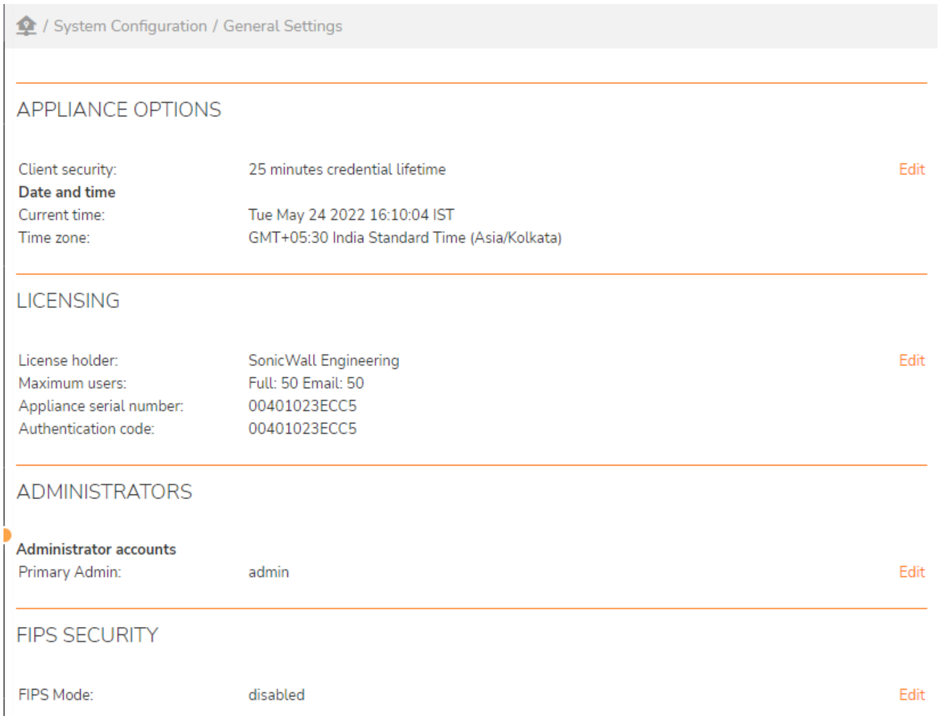
To help keep your AMC password secure, you should change it from time to time. Each administrator can edit his or her own account to change the password or update the description. The primary AMC administrator (whose username is *admin*) can edit the account settings for any other administrator.

Your password must contain between eight and 20 characters, and is case-sensitive. A strong password—with a combination of uppercase and lowercase letters, and numbers—is recommended. You should also avoid using words found in a dictionary.

After you change your password, record it somewhere and keep it secure. If you change a secondary administrator’s password, be sure to share the password with the appropriate administrator.

To edit an administrator account:

1. In the AMC, navigate to **System Configuration > General Settings**.



/ System Configuration / General Settings

APPLIANCE OPTIONS

Client security:	25 minutes credential lifetime	Edit
Date and time		
Current time:	Tue May 24 2022 16:10:04 IST	
Time zone:	GMT+05:30 India Standard Time (Asia/Kolkata)	

LICENSING

License holder:	SonicWall Engineering	Edit
Maximum users:	Full: 50 Email: 50	
Appliance serial number:	00401023ECC5	
Authentication code:	00401023ECC5	

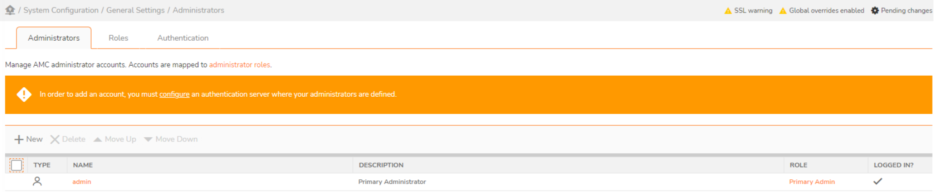
ADMINISTRATORS

Administrator accounts		
Primary Admin:	admin	Edit

FIPS SECURITY

FIPS Mode:	disabled	Edit

2. On the **General Settings** page, in the **Administrator accounts** section, click **Edit**.



Manage AMC administrator accounts. Accounts are mapped to administrator roles.

In order to add an account, you must configure an authentication server where your administrators are defined.

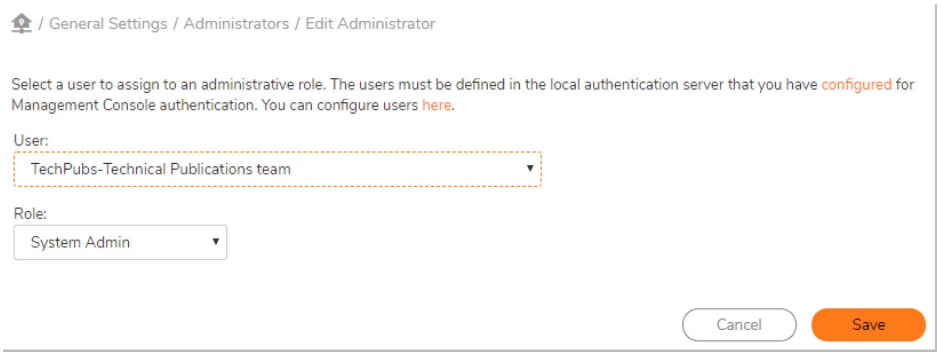
	TYPE	NAME	DESCRIPTION	ROLE	LOGGED IN?
□					
		admin	Primary Administrator	Primary Admin	✓

3. In the **Name** column on the **Administrators** page, click the name of the administrator you want to edit .

ⓘ | **IMPORTANT:** If the password for the primary administrator (whose username is *admin*) is changed, the password for logging in to the appliance directly (as *root*) is also changed.

ⓘ | **NOTE:** The username and role of the primary or legacy local administrator cannot be changed.

4. On the **Edit Administrator** page, change the role of selected administrators.



/ General Settings / Administrators / Edit Administrator

Select a user to assign to an administrative role. The users must be defined in the local authentication server that you have configured for Management Console authentication. You can configure users here.

User: TechPubs-Technical Publications team

Role: System Admin

Editing Administrator Roles

The primary AMC administrator can modify any secondary administrator role to change permission levels, and can also delete secondary roles. For more information, see Defining Administrator Roles.

Defining Administrator Roles

Role-based administration enables the primary administrator to grant limited administrative control to secondary AMC administrators.

For defining administrator roles, the features in AMC are grouped into four categories. For each category, you must specify the permissions you want to grant a role. The four categories of administrator permissions in AMC are described in the below table. The permission level for each category can be set as shown in the Permission levels table.

Administrator Permissions

Category	Administrator permissions
Security administration	Controls administrator access to pages for access control rules, resources, users and groups, WorkPlace, OnDemand, and End Point Control.
System configuration	Controls administrator access to pages for network settings, general appliance settings, SSL settings, access and network services, authentication servers, and realms.
System maintenance	Controls administrator permission to shut down or restart the appliance, update or roll back the system software, and import or export configuration data.
System monitoring	**View** access permits the administrator to view system logs and graphs, view active users, and run troubleshooting tools (such as starting, stopping, downloading, and deleting network traces). **Modify** provides additional permissions to terminate user sessions and modify log settings.

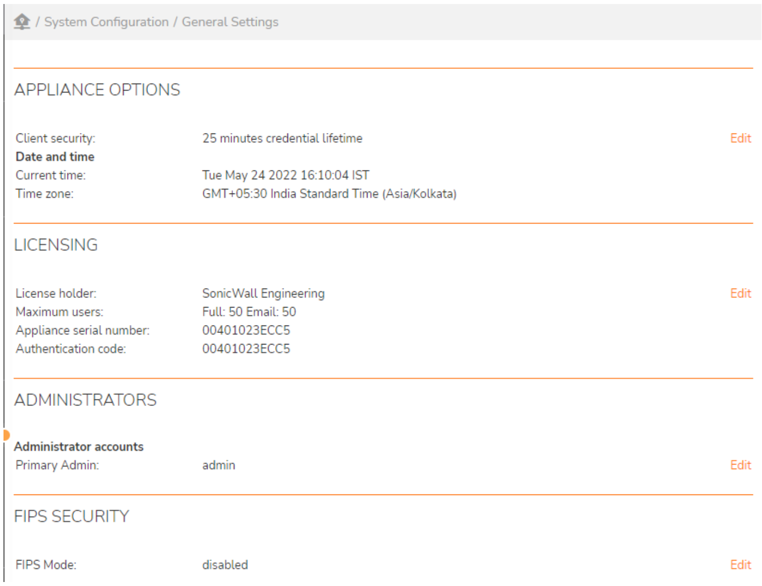
Permission Levels

Permission level	Description
Modify	Permits read/write access within a category.

View	Provides read-only access within a category.
None	Disables access to the relevant AMC pages within a category. When you select **None** as the permission level for a category, AMC does not display either the pages within that category or the main navigation menu commands that lead to those pages.

To create an administrator role:

1. In the AMC, navigate to **System Configuration > General Settings**.



/ System Configuration / General Settings

APPLIANCE OPTIONS

Client security:	25 minutes credential lifetime	Edit
Date and time		
Current time:	Tue May 24 2022 16:10:04 IST	
Time zone:	GMT+05:30 India Standard Time (Asia/Kolkata)	

LICENSING

License holder:	SonicWall Engineering	Edit
Maximum users:	Full: 50 Email: 50	
Appliance serial number:	00401023ECC5	
Authentication code:	00401023ECC5	

ADMINISTRATORS

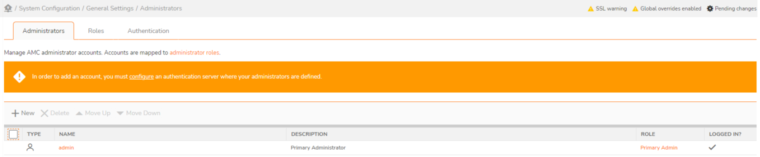
Administrator accounts		
Primary Admin:	admin	Edit

FIPS SECURITY

FIPS Mode:	disabled	Edit

2. In the **Administrators** section, click **Edit** for the **Administrator accounts**.

   The **Administrators** page displays and lists the administrators and their roles.



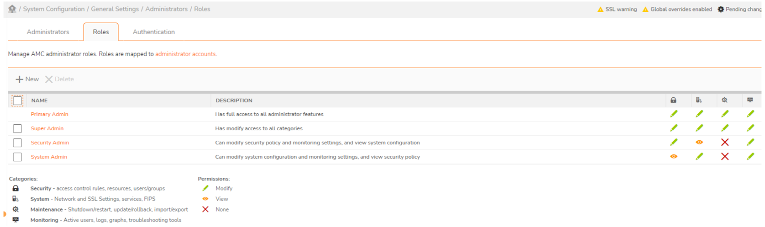
/ System Configuration / General Settings / Administrators

Manage AMC administrator accounts. Accounts are mapped to administrator roles.

In order to add an account, you must configure an authentication server where your administrators are defined.

□	TYPE	NAME	DESCRIPTION	ROLE	LOGGED IN?
		admin	Primary Administrator	Primary Admin	✓

3. Click the **Roles** tab.



/ System Configuration / General Settings / Administrators / Roles

Manage AMC administrator roles. Roles are mapped to administrator accounts.

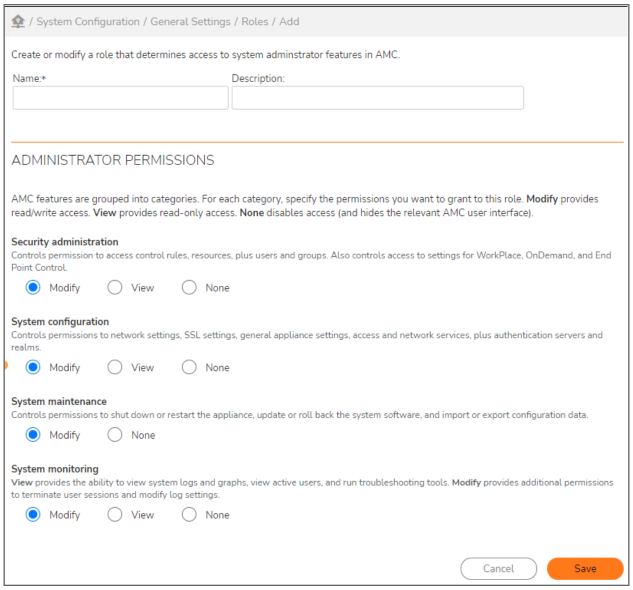
□	NAME	DESCRIPTION	🔒	▤	⚙	🖥
	Primary Admin	Has full access to all administrator features	✎	✎	✎	✎
□	Super Admin	Has modify access to all categories	✎	✎	✎	✎
□	Security Admin	Can modify security policy and monitoring settings, and view system configuration	✎	👁	✗	✎
□	System Admin	Can modify system configuration and monitoring settings, and view security policy	👁	✎	✗	✎

Categories:
- 🔒 **Security** - access control rules, resources, users/groups
- ▤ **System** - Network and SSL Settings, services, FIPS
- ⚙ **Maintenance** - Shutdown/restart, update/rollback, import/export
- 🖥 **Monitoring** - Active users, logs, graphs, troubleshooting tools

Permissions:
- ✎ Modify
- 👁 View
- ✗ None

4. Click the **+** (New) icon.

   The **Add Administrator Role** page displays.



/ System Configuration / General Settings / Roles / Add

Create or modify a role that determines access to system adminstrator features in AMC.

Name:*

Description:

ADMINISTRATOR PERMISSIONS

AMC features are grouped into categories. For each category, specify the permissions you want to grant to this role. **Modify** provides read/write access. **View** provides read-only access. **None** disables access (and hides the relevant AMC user interface).

Security administration
Controls permission to access control rules, resources, plus users and groups. Also controls access to settings for WorkPlace, OnDemand, and End Point Control.

● Modify ○ View ○ None

System configuration
Controls permissions to network settings, SSL settings, general appliance settings, access and network services, plus authentication servers and realms.

● Modify ○ View ○ None

System maintenance
Controls permissions to shut down or restart the appliance, update or roll back the system software, and import or export configuration data.

● Modify ○ None

System monitoring
View provides the ability to view system logs and graphs, view active users, and run troubleshooting tools. **Modify** provides additional permissions to terminate user sessions and modify log settings.

● Modify ○ View ○ None

5. In the **Name** field, type the name for the administrator role.
6. (Optional) In the **Description** field, type a descriptive comment about the role.
7. In the **Administrator permissions** section, select one or more categories of permissions that will be granted to the role.
8. Click **Save**.

API Keys for Management API Access

Many modern RESTful APIs support the use of a key or token for authentication and authorization. The AMC/CMC management API currently supports username/password and API keys using HTTP BASIC authentication. This breaks down when you want to use more complex authentication for AMC, such as chained auth or SAML.

From 12.4.2 onwards, you can use API keys that allows to use the Management API without embedding user credentials in a script. API keys can be used to provide access to scripts when two-factor authentication is required for AMC access.

ⓘ | **NOTE:**

- The system supports a maximum of 10 API keys per administrator.
- The Primary Admin roles can add/remove/modify API keys for all administrators.
- From 12.4.3, non-primary admins also can add/remove/modify their own API keys.
- API keys cannot be assigned to administrators that are groups (local or mapped groups)
- If the request includes both Authorization and X-API-Key headers, only the X-API-Key header will be used.
- An API Key can optionally be made more restrictive than the role assigned to the user using Custom Permission while adding a new API Key. If the actual role becomes more restrictive, then the role

permissions will take precedence and not the custom permissions.

- The key value is displayed/returned only when:
  - Creating a new API key
  - Regenerating the value on an existing key

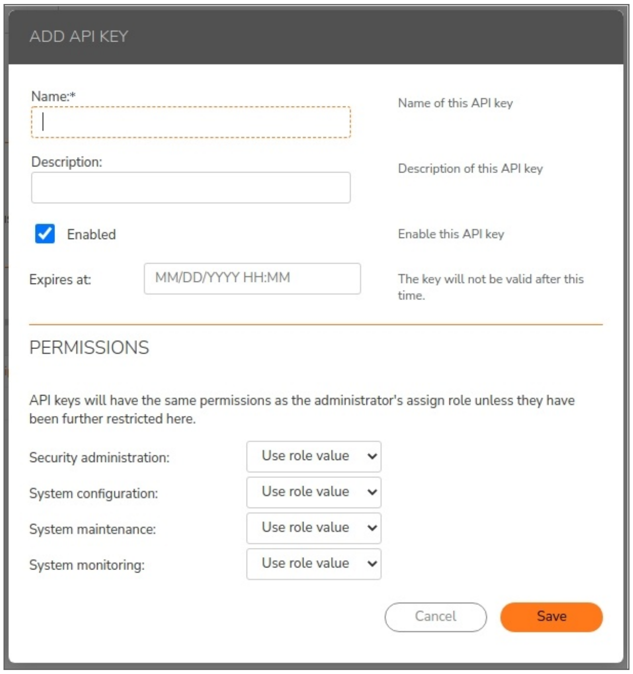
Topics:

- Adding API Keys
- Modifying API key
- Regenerating API key value
- Deleting API key
- Usage of API Keys to access Management API

Adding API Keys

To add a API key:

1. In the AMC, navigate to **System Configuration** > **General Settings**.
2. On the **General Settings** page, in the **Administrator accounts** section, click **Edit**.
3. Configure different type of Admin accounts like Super Admin or Security Admin or System Admin. See Defining Administrator Roles.
4. Click on any of the Administrator.
5. Under **API Keys**, click on **New** to add a new API key for that Administrator.



ADD API KEY

Name:* — Name of this API key

Description: — Description of this API key

☑ Enabled — Enable this API key

Expires at: MM/DD/YYYY HH:MM — The key will not be valid after this time.

PERMISSIONS

API keys will have the same permissions as the administrator's assign role unless they have been further restricted here.

Security administration:	Use role value
System configuration:	Use role value
System maintenance:	Use role value
System monitoring:	Use role value

6. In the **Name** field enter the API key name.
7. In the **Description** field enter description of the API key.
8. Enable the **Enabled** to enable the API key.
9. In the **Expires at** filed set the key validity in the MM/DD/YYYY HH:MM format.
10. Set the administrator **Permissions**.

    NOTE: Re-enter the admin password before clicking on **Save**, if trying to add API key to the Primary Administrator account.

11. Click **Save**.

    The **API Key Values** page is displayed.

12. Copy and save this API Key value.

    NOTE: Once this message is dismissed, the values cannot be recovered.

13. Click **OK**.

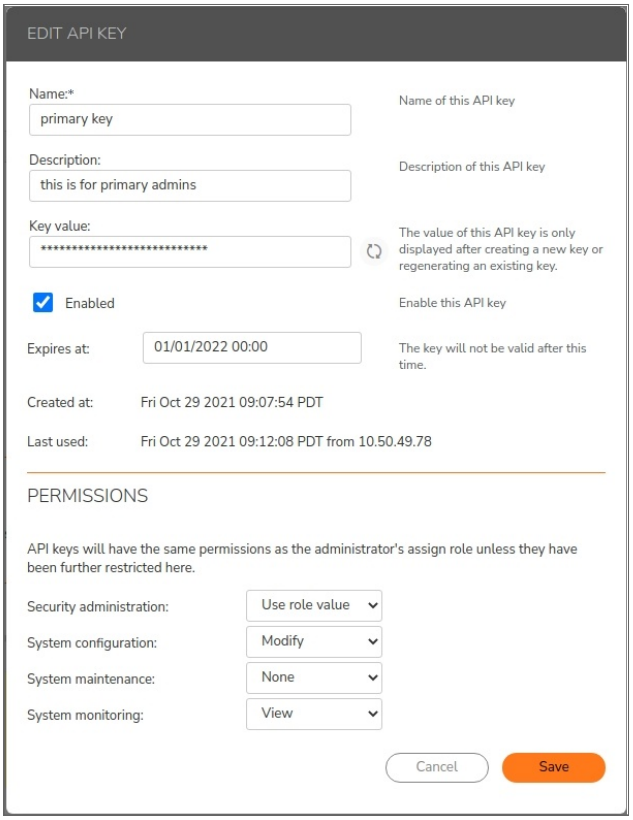
The API Key is now available for Management API Access.

Modifying API key

NOTE: The Primary Admin roles can add or or modify or remove the API keys for all administrators.

To modify a API key:

1. In the AMC, navigate to **System Configuration** > **General Settings**.
2. On the **General Settings** page, in the **Administrator accounts** section, click **Edit**.
3. Configure different type of Admin accounts like Super Admin or Security Admin or System Admin. See Defining Administrator Roles.
4. Click on any of the Administrator.
5. Under **API Keys**, select the API key you want to edit.



EDIT API KEY

Name:* primary key — Name of this API key

Description: this is for primary admins — Description of this API key

Key value: *************************** — The value of this API key is only displayed after creating a new key or regenerating an existing key.

☑ Enabled — Enable this API key

Expires at: 01/01/2022 00:00 — The key will not be valid after this time.

Created at: Fri Oct 29 2021 09:07:54 PDT

Last used: Fri Oct 29 2021 09:12:08 PDT from 10.50.49.78

PERMISSIONS

API keys will have the same permissions as the administrator's assign role unless they have been further restricted here.

Security administration:	Use role value
System configuration:	Modify
System maintenance:	None
System monitoring:	View

6. In the **Name** field enter the API key name.
7. In the **Description** field enter description of the API key.
8. In the **Key value** field you can leave as default with self-generated value or you can re-generate the key value. See Regenerating API Key value.
9. Enable the **Enabled** to enable the API key.
10. Set the administrator **Permissions**.

    ⓘ | **NOTE:** Re-enter the admin password before clicking on **Save**, if trying to add API key to the Primary Administrator account.

11. Click **Save**.

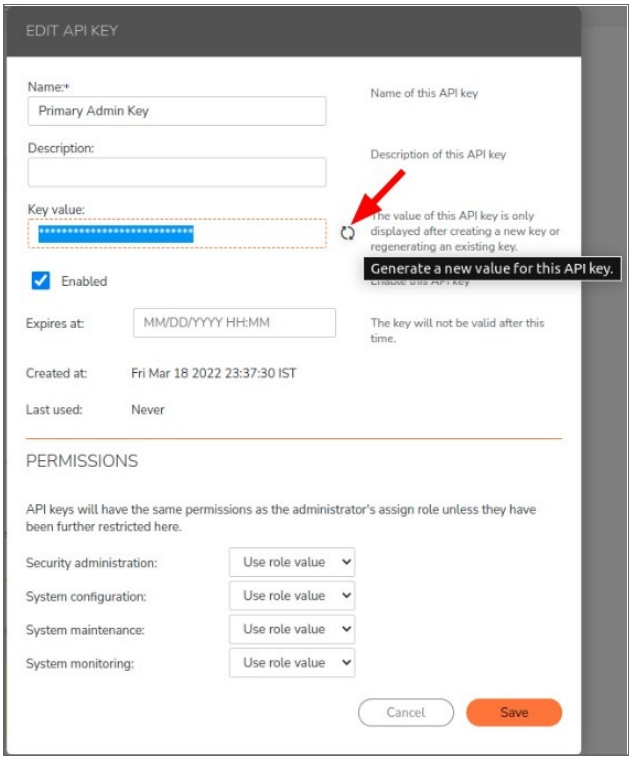
Regenerating API key value

ⓘ | **NOTE:** The Primary Admin roles can add or or modify or remove the API keys for all administrators.

To modify a API key:

1. In the AMC, navigate to **System Configuration** > **General Settings**.
2. On the **General Settings** page, in the **Administrator accounts** section, click **Edit**.
3. Configure different type of Admin accounts like Super Admin or Security Admin or System Admin. See Defining Administrator Roles.

4. Click on any of the Administrator.
5. Under **API Keys**, select the API key you want to re-generate key value.
6. In the **Name** field enter the API key name.
7. In the **Description** field enter description of the API key.



EDIT API KEY

Name:* Primary Admin Key — Name of this API key

Description: — Description of this API key

Key value: ************************** — The value of this API key is only displayed after creating a new key or regenerating an existing key.

Generate a new value for this API key.

☑ Enabled — Enable this API key

Expires at: MM/DD/YYYY HH:MM — The key will not be valid after this time.

Created at: Fri Mar 18 2022 23:37:30 IST

Last used: Never

PERMISSIONS

API keys will have the same permissions as the administrator's assign role unless they have been further restricted here.

Security administration:	Use role value
System configuration:	Use role value
System maintenance:	Use role value
System monitoring:	Use role value

8. In the **Key value** field click the re-generate button to generate a new value for the selected API key.
9. Enable the **Enabled** to enable the API key.
10. Set the administrator **Permissions**.

    ⓘ | **NOTE:** Re-enter the admin password before clicking on **Save**, if trying to add API key to the Primary Administrator account.

11. Click **Save**.

    The **API Key Values** page is displayed.

12. Copy and save this API Key value.

    ⓘ | **NOTE:** Once this message is dismissed, the values cannot be recovered.

13. Click **OK**.

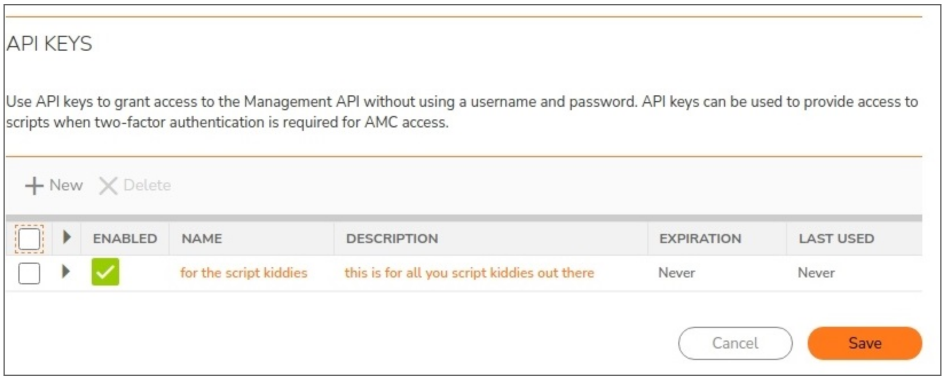
    The API Key is now available for Management API Access.

Deleting API key

ⓘ | **NOTE:** The Primary Admin roles can add or or modify or remove the API keys for all administrators.

To delete a API key:

1. In the AMC, navigate to **System Configuration** > **General Settings**.
2. On the **General Settings** page, in the **Administrator accounts** section, click **Edit**.
3. Configure different type of Admin accounts like Super Admin or Security Admin or System Admin. See Defining Administrator Roles.
4. Click on any of the Administrator.
5. Under **API Keys**, select the API key you want to delete.



API KEYS

Use API keys to grant access to the Management API without using a username and password. API keys can be used to provide access to scripts when two-factor authentication is required for AMC access.

□		ENABLED	NAME	DESCRIPTION	EXPIRATION	LAST USED
□	▸	✓	for the script kiddies	this is for all you script kiddies out there	Never	Never

6. Click **Delete**.

Usage of API Keys to access Management API

Client authenticates API request with custom HTTP header X-API-Key. Each HTTP request must contain either a Authorization header with log in credentials username:password encoded in Base64 or an X-API-key header with a valid API key.

For Example:

- Authorization: `Basic QwxhZGRpbjpvcGVuIHN1c2FtZQ==`
- X-API-Key: `20b1b203-0b41-4ef9-8db7-1117e99dc08c`

API Key used in Curl Example:

Client authenticates API request with custom HTTP header X-API-Key

Example:

```
curl -k -H "X-API-Key:9fc53abb-0041-47eb-afc4-9ed08e23ff2f" https:// x.x.x.x
:8443/Console/SSH
```

Managing Administrator Account Settings

Secure Mobile Access allows you to choose the authentication server where your appliance administrators are defined. If you do not already have accounts defined in an external directory server, you can create a local authentication store and assign administrative roles to locally defined users and groups.

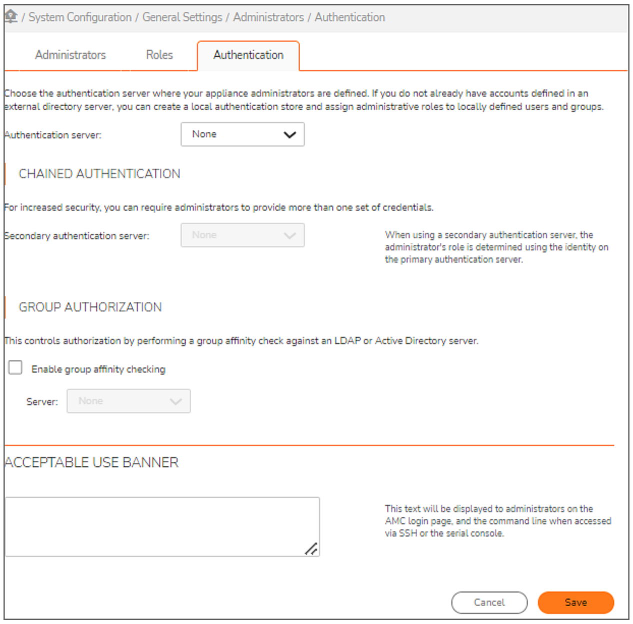
The SMA100012.4.3 allows you to do the following:

- Adding Authentication Server
- Configuring Password Policy
- Configuring Account Lockout
- Configuring Session Timeout
- Configuring Concurrent Sessions

Adding Authentication Server

To add an authentication server:

1. See the Configuring Authentication Servers section to add the authentication servers.
2. Navigate to **System Configuration** >**General Settings**.
3. In the **Administrators** area, click **Edit** for the Administrator accounts.
4. Click the **Authentication** tab.



Choose the authentication server where your appliance administrators are defined. If you do not already have accounts defined in an external directory server, you can create a local authentication store and assign administrative roles to locally defined users and groups.

Authentication server: None

For increased security, you can require administrators to provide more than one set of credentials.

Secondary authentication server: None

When using a secondary authentication server, the administrator's role is determined using the identity on the primary authentication server.

This controls authorization by performing a group affinity check against an LDAP or Active Directory server.

☐ Enable group affinity checking

Server: None

This text will be displayed to administrators on the AMC login page, and the command line when accessed via SSH or the serial console.

5. In the **Authentication server** drop-down menu, select the authentication server you added in *Step 2*.
6. Keep all other options as default.
7. Click **Save**.
8. Click **Pending Changes** in the upper-right of the page.
9. Click **Apply Changes**.

Configuring Password Policy

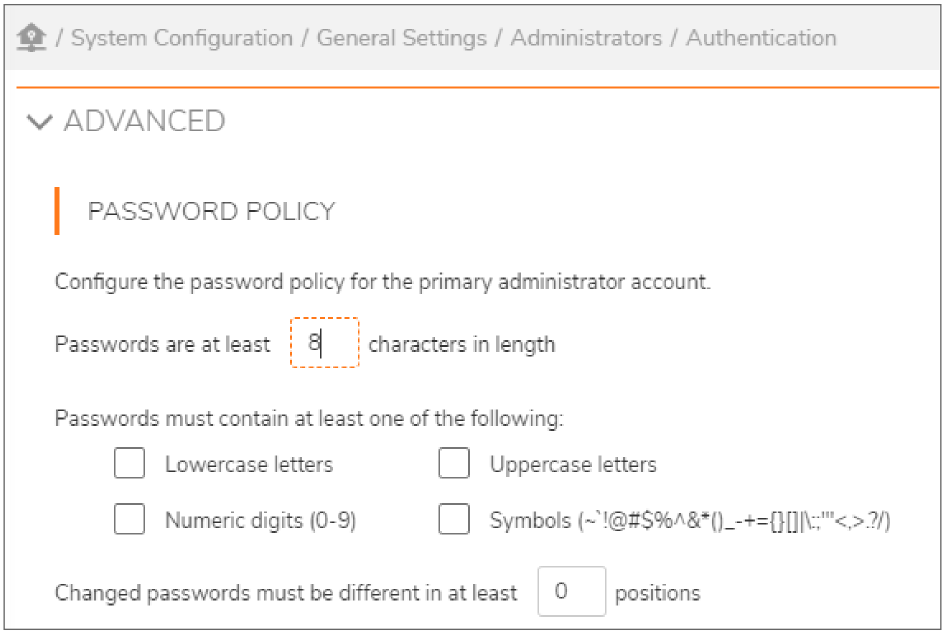
The SMA1000 12.4.3 provides strong password complexity settings for the primary administrator account.

Prerequisites:

- SMA/CMS running 12.4.3 firmware version.

To configure the password policy for the primary administrator account:

1. In AMC, navigate to **System Configuration** > **General Settings**.
2. In the **Administrators** area, click **Edit** for the Administrator accounts.
3. Click the **Authentication** tab.
4. Go to **Advanced** > **Password Policy** section.
5. Enter the minimum number of characters allowed for passwords. The minimum can be eight.



/ System Configuration / General Settings / Administrators / Authentication

ADVANCED

PASSWORD POLICY

Configure the password policy for the primary administrator account.

Passwords are at least 8 characters in length

Passwords must contain at least one of the following:

□ Lowercase letters □ Uppercase letters

□ Numeric digits (0-9) □ Symbols (~`!@#$%^&*()_-+={}[]|\:;'"<,>.?/)

Changed passwords must be different in at least 0 positions

6. Select the password policy criteria options.

Option	Description
Lowercase	To specify that user passwords must contain at least one lowercase character
Uppercase	To specify that user passwords must contain at least one uppercase character.
Numeric digits (0-9)	To specify that user passwords must contain at least one number (0-9).
Symbols	To specify that user passwords must contain at least one symbolic character (~`!@#$%^&*()_-+={}[]|\:;'"<,>.?/).

7. Specify the positions to prevent changing your new password to be similar to older password in the **Changed password must be different in at least** field. For example, to prevent from changing the password from mypass1 to mypass2.
8. Click **Save**.

Configuring Account Lockout

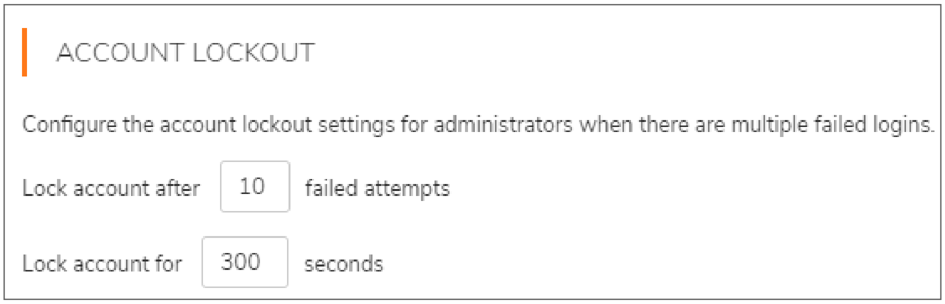
The SMA1000 12.4.3 provides the **Account lockout** settings for administrators when there are multiple failed login attempts.

Prerequisites:

- SMA/CMS running 12.4.3 firmware version.

To configure the account lockout for the primary administrator account:

1. In AMC, navigate to **System Configuration** > **General Settings**.
2. In the **Administrators** area, click **Edit** for the Administrator accounts.
3. Click the **Authentication** tab.
4. Go to **Advanced** > **Account Lockout** section.



ACCOUNT LOCKOUT

Configure the account lockout settings for administrators when there are multiple failed logins.

Lock account after 10 failed attempts

Lock account for 300 seconds

5. Enter the **Lock account** after how many failed login attempts. The value must be not less than 2 and not greater than 100.
6. Enter the **Lock account for** how many seconds after the failed login attempts. The value must be not less than 10 and not greater than 3600.
7. Click **Save**.

Configuring Session Timeout

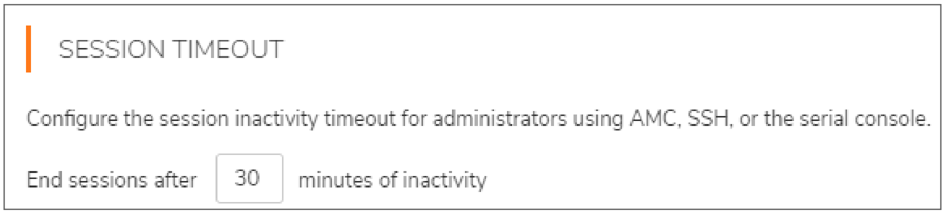
The SMA1000 12.4.3 provides **Session timeout** settings for administrators to configure the session inactivity timeout.

Prerequisites:

- SMA/CMS running 12.4.3 firmware version.

To configure session timeout:

1. In AMC, navigate to **System Configuration** > **General Settings**.
2. In the **Administrators** area, click **Edit** for the Administrator accounts.
3. Click the **Authentication** tab.
4. Go to **Advanced** > **Session Timeout** section.



SESSION TIMEOUT

Configure the session inactivity timeout for administrators using AMC, SSH, or the serial console.

End sessions after 30 minutes of inactivity

5. Enter the number of minutes of on inactivity after which an AMC, SSH, or console session will be terminated. The value must be not less than 1 and not greater than 720.
6. Click **Save**.

Configuring Concurrent Sessions

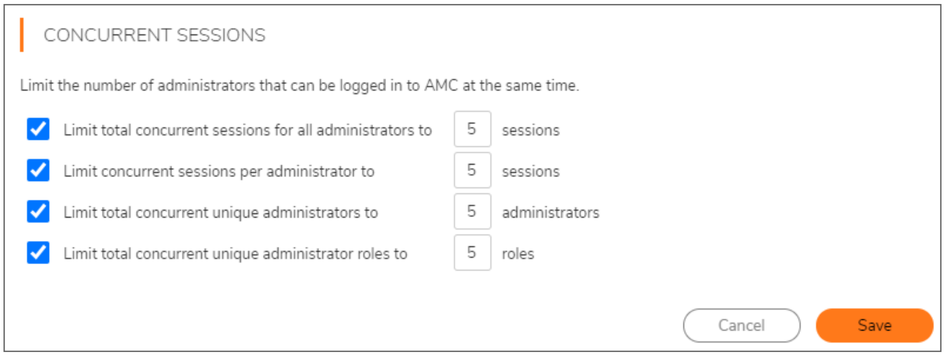
The SMA100012.4.3 provides **Concurrent Session** settings for administrators to configure the concurrent session to limit the number of sessions and admins that can be logged in to AMC by either identity (for example, username) or role (for example, super admin).

Prerequisites:

- SMA/CMS running 12.4.3 firmware version.

To configure concurrent session:

1. In AMC, navigate to **System Configuration** > **General Settings**.
2. In the **Administrators** area, click **Edit** for the Administrator accounts.
3. Click the **Authentication** tab.
4. Go to **Advanced** > **Concurrent Session** section.



CONCURRENT SESSIONS

Limit the number of administrators that can be logged in to AMC at the same time.

☑ Limit total concurrent sessions for all administrators to 5 sessions

☑ Limit concurrent sessions per administrator to 5 sessions

☑ Limit total concurrent unique administrators to 5 administrators

☑ Limit total concurrent unique administrator roles to 5 roles

5. Enter the following concurrent sessions to limit the sessions and admins.

ⓘ | **NOTE:** The limit values must be a number not less than 1 and not greater than 20.

Option	Description
Limit total concurrent sessions for all administrators	Limits the total number of admin sessions that can be logged in to AMC at the same time, regardless of which user is logged in.

Option	Description
Limit concurrent sessions per administrator	Limits the number of AMC sessions that one admin user can have at the same time. Does not limit the total number of admins or total number of sessions.
Limit total concurrent unique administrators	Limits the number of unique admin users that can be logged in to AMC at the same time. Does not limit the number of sessions that a single user can have at the same time.
Limit total concurrent unique administrator roles	Limits the number of unique admin roles that can be logged in to AMC at the same time. Does not limit the number of sessions per role.

6. Click **Save**.

Avoiding Configuration Conflicts with Multiple Administrators

If more than one administrator is managing your appliance, you should avoid working in AMC at the same time. If multiple administrators make changes to the same object, AMC saves the most recent one. This can cause unintentional results, and potentially cause security problems if conflicting changes are made to access control rules.

If more than one administrator is logged into AMC, you are alerted by a link in the upper-right corner of AMC.

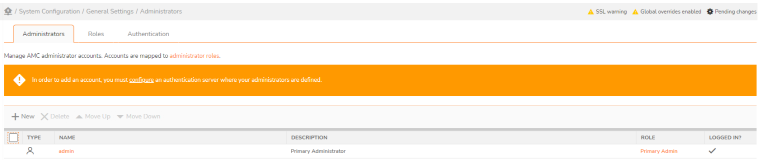
To see a list of the user names and IP addresses of all administrators who are logged into AMC, click this link: the **Administrator Sessions** page displays in a separate window. If an administrator has multiple instances of the Web browser logged into AMC, the administrator's user name and IP address is listed more than once.

You should contact the other administrators and coordinate your activities to avoid configuration conflicts.

To view the complete list of AMC administrators:

1. In the AMC, navigate to **System Configuration > General Settings**.
2. Click **Edit** in the **Administrator accounts** area.

   The **Administrators** page lists all administrators and shows which ones are currently logged in.



Manage AMC administrator accounts. Accounts are mapped to administrator roles.

In order to add an account, you must configure an authentication server where your administrators are defined.

□	TYPE	NAME	DESCRIPTION	ROLE	LOGGED IN?
		admin	Primary Administrator	Primary Admin	✓

The management console audit log tracks any AMC configuration changes made by administrators. See Management Audit Log.

To end an AMC session you must click **Log Out**; if you terminate a session by closing your Web browser, the session appears in the list of active sessions until it times out (by default, in 15 minutes).

Managing Multiple Secure Mobile Access Appliances

SMA appliances should be managed by the Central Management Server (CMS).

ⓘ | **IMPORTANT:** GMS is not supported in SMA 12.4.

The Central Management Server (CMS) is a single administrative user interface from which you can manage all of your VPN appliances. CMS is a virtual machine that reduces the total cost of operation and simplifies the management of multiple VPN appliances for enterprise companies.

Central Management Server (CMS)

The VPN administrator uses the Central Management Console (CMC) of the CMS to manage all the VPN appliances regardless of location. CMS and managed appliances are closely integrated through native communications secured with TLS.

Central Management:

- Provides enterprise customers a Dashboard to manage their distributed VPN infrastructure.
- Reduces Total Cost of Operation (TCO) and operator errors associated with the management of multiple appliances.
- Provides a Central Management Console (CMC) to configure, maintain and monitor appliances.
- Simplifies license management with a centralized license that eliminates the need for separate appliance licenses.
- Facilitates centralized alerts via the console dashboard and SNMP traps.
- Requires no dedicated appliance or hardware (The Central Management Server is a virtual machine).

The dashboard view in the CMC gives you a summarized view of all managed appliances.

You can apply a common configuration to managed appliances from the CMC. Consolidated monitoring and reporting gives the Administrator an overview of all the appliances that are being managed.

For more information about using the CMS, see the *Secure Mobile Access 12.4.1 Central Management Server Administration Guide*.

Working with Configuration Data

This section explains how to save and activate configuration changes in AMC.

Topics:

Saving Configuration Changes

When you’re finished making changes on a page in AMC and you click **Save**, your changes are saved. If you click **Cancel** or use the Back button in your browser, your changes are not saved.

To save configuration changes to disk:

1. Make any changes on a page in AMC.
2. Click **Save** at the bottom of the page.

Configuration changes are saved, but are not applied to the active configuration. The status area in AMC changes to indicate that you have pending changes that need to be applied to the appliance.

See Applying Configuration Changes for more information.

There are several options for managing configuration data—exporting it or saving it on the appliance, or restoring it, for example. See Managing Configuration Data for more information.

Applying Configuration Changes

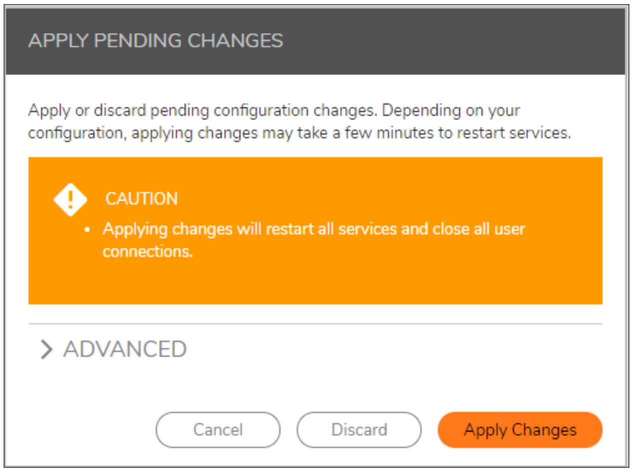
As you make configuration changes to the appliance, they are saved but are not immediately applied. These changes can either be applied (described in this section) or discarded (see Discarding Pending Configuration Changes for more information).

To activate your changes, you must apply them. You can apply most changes without interrupting service to users, and new connections will use the new configuration. Low-level configuration changes (for example, an IP address change) are a bit more disruptive: network services are automatically restarted and user connections are terminated, forcing users to reauthenticate. If possible, you should apply these sorts of configuration changes during off-peak hours (perhaps during a maintenance window) and notify your users beforehand.

If you need to restart services manually, see Stopping and Starting the Secure Mobile Access Services.

To apply your changes:

1. From the list of messages at the top of the page, click **Pending changes**.
   The **Apply Pending Changes** dialog displays.



APPLY PENDING CHANGES

Apply or discard pending configuration changes. Depending on your configuration, applying changes may take a few minutes to restart services.

CAUTION

- Applying changes will restart all services and close all user connections.

2. Assess the impact of applying your changes by looking at the message on the **Apply Changes** page:

Warning message	Description
• Applying changes will restart all services and terminate all user connections. • Applying changes will terminate existing TCP/IP user connections. • Applying changes will terminate existing HTTP user connections.	Applying any of these changes terminates existing user connections. ⚠ **CAUTION: This requires users to reauthenticate, and may cause them to lose data.**
Your changes will require AMC to restart, which will end your current administrative session. When the request is complete, open a new browser and log in to AMC again.	AMC will be unavailable after your current session ends. Close your browser and then log in to AMC again.
No authentication realms are enabled. This will prevent users from accessing any resources.	At least one authentication realm must be enabled for users to have access to resources. Otherwise, users cannot authenticate to the appliance.

3. Click **Apply Changes** to apply configuration changes.

When you apply configuration changes to WorkPlace, AMC performs a restart of the services. Users do not need to reauthenticate to WorkPlace, but if they provided Windows login credentials to access a network share, they are prompted to re-enter them when WorkPlace restarts.

Any connections that exist when you apply changes continue to use the old configuration until the connection terminates. Because Web connections are short-lived, most users accessing Web resources pick up configuration changes fairly quickly. On the other hand, client/server connections can survive for a long period of time.

If the new configuration fails to load, existing connections remain in effect but new connection attempts will fail. For details on what to do in this situation, see AMC Issues.

Discarding Pending Configuration Changes

Configuration changes you make in AMC are saved, but they are not in effect until you apply them, as described in Applying Configuration Changes. You can use the policy audit log file to find out what changes are pending, and go to the **Apply changes** page in AMC to discard them. Pending changes can only be discarded as a group: you cannot discard them selectively.

To discard pending changes:

1. (Optional) You can review the list of pending changes in the management console audit log file.
   a. From the main navigation menu, click **Logging**, and then select **Management Console audit log** in the **Log file** list.
   b. Any **Info** level item added since the last **Applied configuration changes message** appears is a change that can be discarded.

   See Management Audit Log for more information.
2. Click **Pending changes** in the upper right of any page in the AMC.

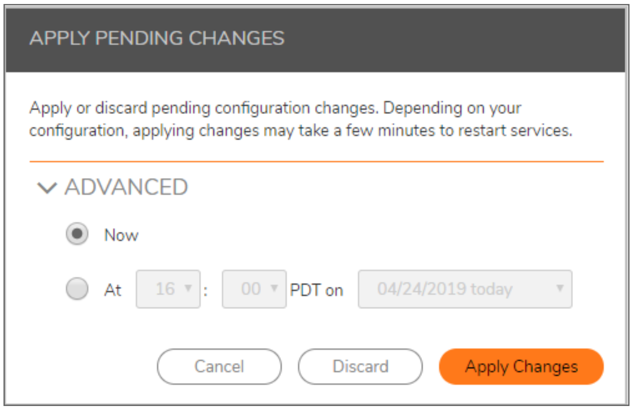
   The **Apply Pending Changes** dialog displays.
3. On the **Apply Changes** page, click **Discard**.

   The changes are discarded.

Scheduling Pending Changes

To schedule changes:

1. Either click the **Pending changes** link in the upper-right corner of AMC to display the **Apply Pending Changes** dialog.
2. Expand the **Advanced** section by clicking the **Down** arrow icon next to the **Advanced** heading.



APPLY PENDING CHANGES

Apply or discard pending configuration changes. Depending on your configuration, applying changes may take a few minutes to restart services.

ADVANCED

● Now

○ At 16 : 00 PDT on 04/24/2019 today

3. To schedule the pending changes to be applied at a later time, click the **At** radio button and select the desired time and date.

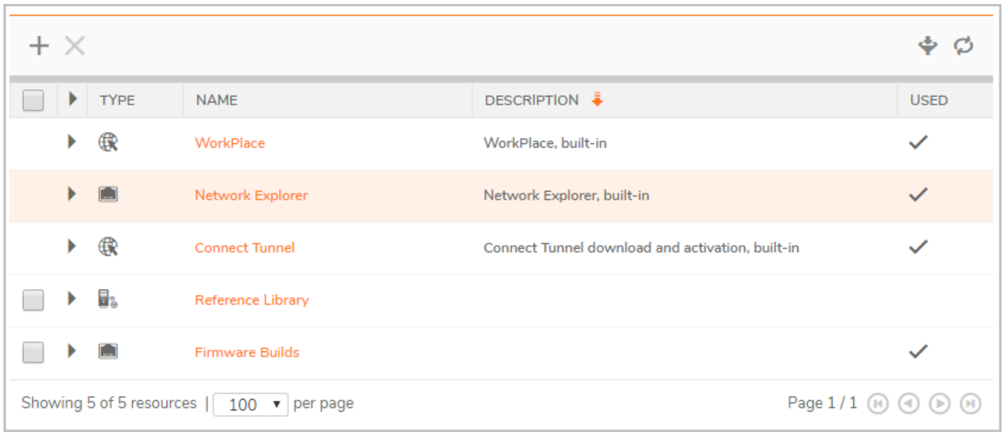
You also may apply the pending changes immediately by selecting the **Now** radio button or discard the pending changes by clicking **Discard**.

4. Click **Apply Changes**. Thereafter, clicking **Pending Changes** displays the scheduled actions.

A schedule can be changed or discarded at any time before the scheduled time using this .

Deleting Referenced Objects

You cannot delete an object (such as a resource or a user) if it is still referenced by another object (the checkbox next to it in AMC cannot be selected) or is a built-in component (such as *Connect Tunnel*).



□		TYPE	NAME	DESCRIPTION	USED
			WorkPlace	WorkPlace, built-in	✓
			Network Explorer	Network Explorer, built-in	✓
			Connect Tunnel	Connect Tunnel download and activation, built-in	✓
□			Reference Library		
□			Firmware Builds		✓

Showing 5 of 5 resources | 100 per page   Page 1 / 1

To delete an object that is in use by anther object—such as a Web shortcut, a WorkPlace layout, or an access rule—you must first out what objects are using it. To do this, expand the list item by clicking on the plus (**+**) sign next to it.

The below table lists the object types that cannot be deleted if they are referenced by other objects.

This object type	Can be referenced by this object type
Resource	Access control rules, resource groups, WorkPlace Web shortcuts
Resource groups	Access control rules
Users	Access control rules
User groups	Access control rules
Realms	Users, user groups
Authentication servers	Realms
Communities	Realms
Web application profiles	Resources
End Point Control zones	Access control rules, communities
Device profiles	End Point Control zones

User Management

Topics:

- Users, Groups, Communities, and Realms
- Using Realms and Communities
- Configuring Realms and Communities
- Integrating an SMA Appliance with a SonicWall Firewall
- Managing Users and Groups

Users, Groups, Communities, and Realms

Access control rules determine which resources are available for users or groups of users. Accordingly, you must define users and groups in AMC that map to users or groups stored in external user directories or in the local user authentication repository on the appliance. At a higher level, communities organize users or user groups that share common characteristics, most notably access policy and access methods, and can also be used in access control rules.

Topics:

- Users and groups
- Communities
- Realms

Users and groups

A user is an individual who needs access to resources on your network, and a group is a collection of users. After you've created users or groups on the appliance, you can reference them in an access control rule to permit or deny access to resources.

Users and groups can be stored on an external authentication server or on the appliance in a local user authentication repository. When an external authentication server, such as LDAP or Microsoft Active Directory, is being used, you create references to existing users or groups stored in that server. These users or groups, as well as local users and groups, are referenced in access control rules to control authorization. You can even query the external directory (looking for users who share certain attributes, for example) and use the results to create a group to use in an access control rule. This is useful when you do not want to create and manage users directly on the appliance.

Creating local users and groups on the appliance is useful to allow external users to access a set of internal company resources, such as a reseller who needs access to a special order status page on an internal system. For deployments without an existing company-wide directory server in place, the local user authentication repository allows group-based policy without the need to install, configure, and maintain another server.

You can define a user or group before referencing it in an access control rule; alternatively, you can define a new user or group directly from the access control rule interface.

Communities

Communities are collections of users that determine which access methods and End Point Control agents are deployed to the members of a user population when they log in to a realm. For example, you may want to enable OnDemand for your mobile employees, but provide only Web access to your business partners. If End Point Control is enabled, communities can also be used to determine which “zones of trust” members belong to.

Realms

A realm references an authentication server and determines which access agents are provisioned to your users and what End Point Control restrictions are imposed based on the communities configured or added.

Using Realms and Communities

When you set up realms and user communities, AMC enables you to specify which access agents are provisioned to members of the communities. You also have the option of classifying community members’ devices into “zones of trust.” The following illustration shows how a realm authenticates users, assigns them to communities to provision access agents and, with End Point Control enabled, assigns community members to different zones based on the trustworthiness of their devices.

If your network uses only one authentication server to store user information, then you probably need to create only one realm in AMC. If your network uses multiple authentication servers, you must create at least one realm for each of them. You can also create multiple realms in AMC that reference separate user populations in a single external repository.

Using only one authentication realm doesn’t limit your ability to create subsets of users based on their access needs or other security considerations, because realms must be associated with communities of users. A community can consist of all users in a realm or only selected users; it is used to deploy access agents and to enforce End Point Control restrictions for members of a community.

Topics:

- Viewing Realms
- Default, Visible, and Hidden Realms
- Specifying the Default Realm
- Enabling and Disabling Realms
- Best Practices for Defining Realms

Viewing Realms

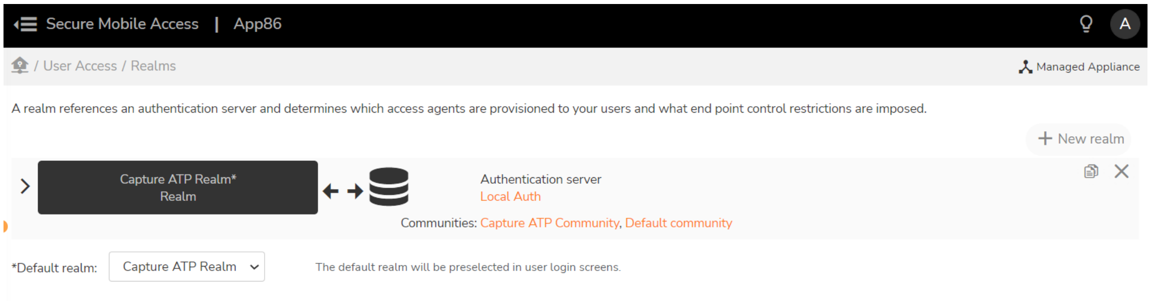
You can view the list of configured realms, including all “building blocks” that are associated with each one: the authentication servers and communities. The communities, in turn, determine who has access using what methods, what security zone to place a device in, based on its profile, and even the appearance of WorkPlace.

To view configured realms:

1. Under **User Access** in the left navigation pane, click **Realms**.

   The **Realms** page displays.

   Collapsed View

   Secure Mobile Access | App86

   / User Access / Realms

   Managed Appliance

   A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

   + New realm

   Capture ATP Realm*
   Realm

   Authentication server
   Local Auth

   Communities: Capture ATP Community, Default community

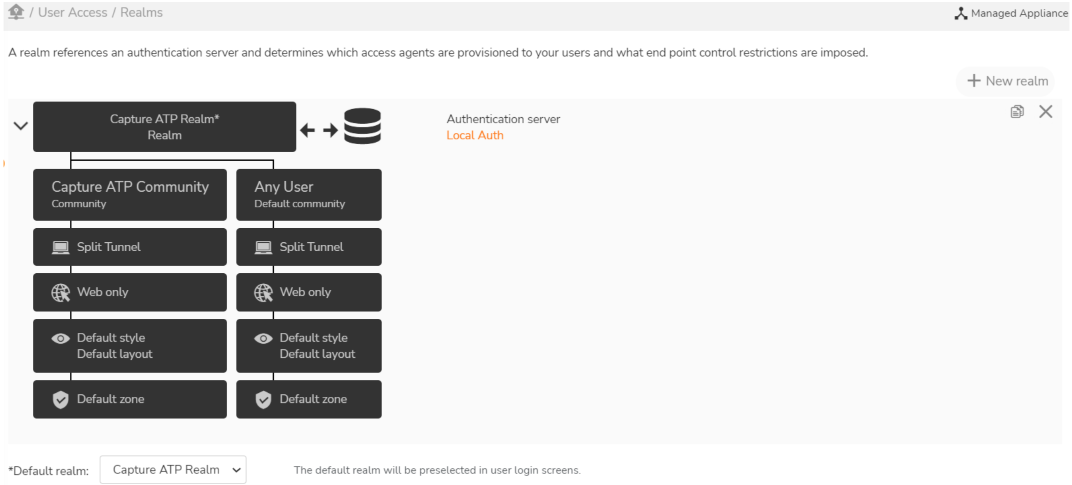
   *Default realm: Capture ATP Realm

   The default realm will be preselected in user login screens.

   The **Collapsed View** gives you a quick summary of each realm. Click any item to go directly to its corresponding configuration page in AMC:

   - Users and groups associated with a disabled realm are unable to log in. See Enabling and Disabling Realms for more details.
   - The **Authentication server** area shows the name or names of the servers that are used by a realm to verify users’ identities. Clicking on the server name displays the **System Configuration > Authentication Servers** page for that server.
   - The (optional) descriptive text you entered when creating a realm is on the right.
   - You can use the:
     - **Up** and **Down** Arrow ▲ ▼ icons to re-order the list of realms.
     - **Copy** ⧉ icon to create a copy of a realm to modify.
     - **Delete** ✕ icon to delete a realm.
   - Below the server information is a list of communities associated with the realm.

Expanded View


/ User Access / Realms

A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

Authentication server: Local Auth

*Default realm: Capture ATP Realm

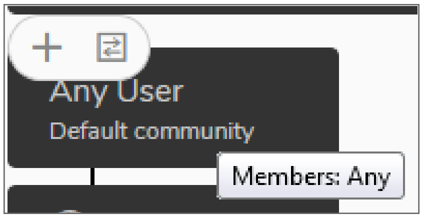
The default realm will be preselected in user login screens.

The **Expanded View** expands the list of communities to graphically represent the Communities, Tunnel Access, Browser Access, Workplace appearance, and Zones.

You can:

- Expand or collapse all realms by clicking on the **Expand all details** or **Collapse all details** link at the top of the page.
- Expand or collapse a single realm by clicking its:
  - **Right Arrow** (›) to see more detail.
  - **Down Arrow** (⌄) to see less detail.

2. Communities allow you to group realm members based on different security needs. For a quick check of which members belong to a community, move the pointer over the community name.

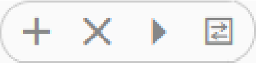


3. You can access the relevant pages for:

   - Default style 👁 – The appearance of the WorkPlace portal is governed by a style and layout that you can configure. If you have a community of mobile device users, for example, you might want to create a more compact look and layout for it.
   - Tunnel Access 💻 – Lists the tunnel access method(s) for the community.

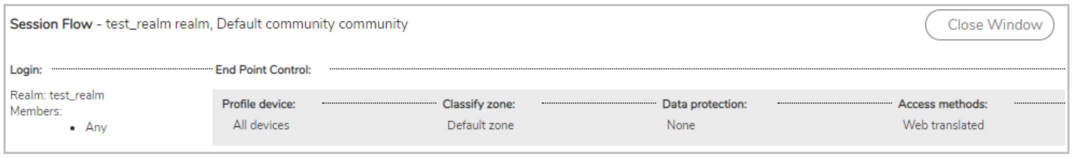
- Browser Access 🌐 – Lists the browser access method(s) for the community.
- Security Zone ✓ – Are used to allow or deny access using device profiles. For a quick check of which device profiles are used by a particular zone, move the pointer over the zone name.

4. There are a number of community-level configuration changes you can make on this page in AMC. Move the cursor over a community name:

   Using the controls that appear when you are positioned over a community, you can:

   - Add or delete a community with the **Add**(**+**) or **Delete** (**X**) icons.
   - Change the order in which users are grouped by moving the community left or right with the **Right** (**>**) or **Left** (**<**) **Arrow** icons.
   - To see the session workflow, move the pointer over the community name and click the **Session Flow** ⇄ icon.

   Session Flow - test_realm realm, Default community community

   Close Window

   Login:

   Realm: test_realm
   Members:
   - Any

   End Point Control:

Profile device:	**Classify zone:**	**Data protection:**	**Access methods:**
All devices	Default zone	None	Web translated

5. Specify a default realm from the **Default realm** drop-down menu (at the bottom of the page), which lists all the displayed realms.

   The default realm is preselected in user login screens.

Default, Visible, and Hidden Realms

To authenticate a user, the appliance must know which realm the user belongs to. If only one realm is enabled, the appliance automatically uses it. However, if multiple realms are enabled, the appliance needs to know which one to use.

When users log in, they typically select the appropriate realm from a list. You can make the choice easier for them by defining a default realm in AMC (see Specifying the Default Realm for more information). If a default realm is defined, the realm selection field is automatically populated with that realm. The specific behavior of each access method is outlined in this section.

ⓘ | **IMPORTANT:** SonicWall strongly recommends that you specify a default realm.

You can also choose which realm names are visible to users. If a realm is hidden, the user must know its name and manually type it during login. For example, you could create realms for various suppliers. If you'd prefer that they not know about one another, you could configure the realm names to be hidden. Each supplier then has to type the realm name when logging in to the appliance.

For the typical user login experience for various realm configurations, see below table.

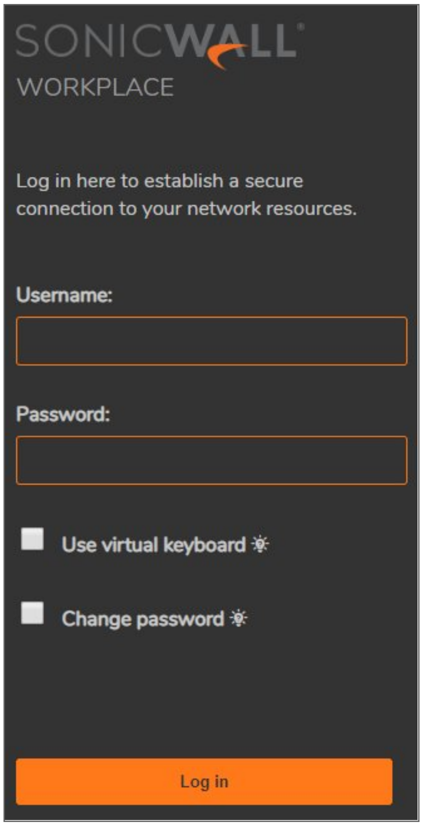
Typical User Login Experience For Various Realm Configurations

Realms enabled	Default realm configured?	Hidden realms configured?	User's login experience
One	N/A	N/A	User does not need to select a realm during the login process. Access methods automatically use the one enabled realm for authentication.
Multiple	Yes	None	User selects a realm from the list. The **Realm** field is initially populated with the default realm.
Multiple	Yes	Yes	User selects a realm from the list. The **Realm** field is initially populated with the default realm. If login requires a hidden realm, user selects **Other** and then types the realm name in a second field.

When users first access Secure Mobile Access WorkPlace, they are presented with one or more login pages. If only one realm is enabled, they see only the page requesting their user credentials. If multiple realms are enabled, they see a login page on which they select the appropriate realm from a drop-down menu. The default realm selected on the **User Access > Realms** page is displayed as the preselected realm in the drop-down menu. If there are one or more hidden realms, the login page prompts the user to type in the realm name.

ⓘ **NOTE:** Up to 200 realms can be defined for users to choose from. As an alternative, to avoid manual selection, WorkPlace sites can be set up with a unique realm configured for each WorkPlace site. The default number of Workplace sites is **200**.

After clicking **Next**, users authenticating with user name and password are presented with the page for entering credentials.



Log in here to establish a secure connection to your network resources.

Specifying the Default Realm

If you specify more than one authentication realm, you must designate one as the default. To authenticate a user, the appliance must know which realm the user belongs to. If only one realm is enabled, the appliance automatically uses it. If multiple realms are enabled, the appliance needs to know which one to use. A user can select the appropriate one from a list, but the process is easier for the user if you designate a default realm in AMC. (Even if you configure only one realm, you should specify it as the default; otherwise AMC displays the warning message, `There is no default realm selected`, on the **Realms** page.)

To specify a default realm:

1. In the AMC, navigate to **User Access > Realms**.
2. In the **Default realm** list (at the bottom of the AMC page), select the authentication realm that will be the default.

   This list shows only those realms that are enabled and configured to be displayed.

Enabling and Disabling Realms

The appliance supports the simultaneous use of multiple realms. You can control which realms are active by enabling and disabling them. When a realm is disabled, users and groups associated with that realm are unable to log in. If no authentication realm is enabled, users do not have access to the network.

To enable or disable an authentication realm:

1. In the AMC, navigate to **User Access > Realms** to view the list of defined realms.

   If a realm is disabled, the realm is grayed out.
2. Click the name of the realm you want to enable or disable.

   This displays the **Configure Realm** page for that realm.
3. In the **General** area, select whether the **Status** for the realm is **Enabled** or **Disabled**.
4. Click **Save**.

Best Practices for Defining Realms

When defining realms, follow these best practices to simplify your users' login experience.

- Your users select a realm name when logging in, so define realm names that clearly describe the user population. For example, a realm that includes all internal employees might be named "employees," while a realm that includes external suppliers might be named "suppliers."

  If a realm will be referenced by mobile device users, keep the name short so that all of it is visible on the mobile device.
- If some users will be logging in to a realm that is hidden, make sure they know the name of the realm and how to type it in (choose **Other** from the realm list and then type the realm name in the field).
- Enable multiple realms only if necessary. If only one realm is enabled, users do not need to select a realm as part of the login process. When moving from a test to a production environment, verify that all test realms have been removed.

Configuring Realms and Communities

Topics:

- Creating Realms
- Adding Communities to a Realm
- Creating and Configuring Communities
- Network Tunnel Client Configuration
- Using the Default Community
- Changing the Order of Communities Listed in a Realm
- Configuring RADIUS Accounting in a Realm
- Configuring an SMA Appliance to Send RADIUS Accounting Records to a Firewall

Creating Realms

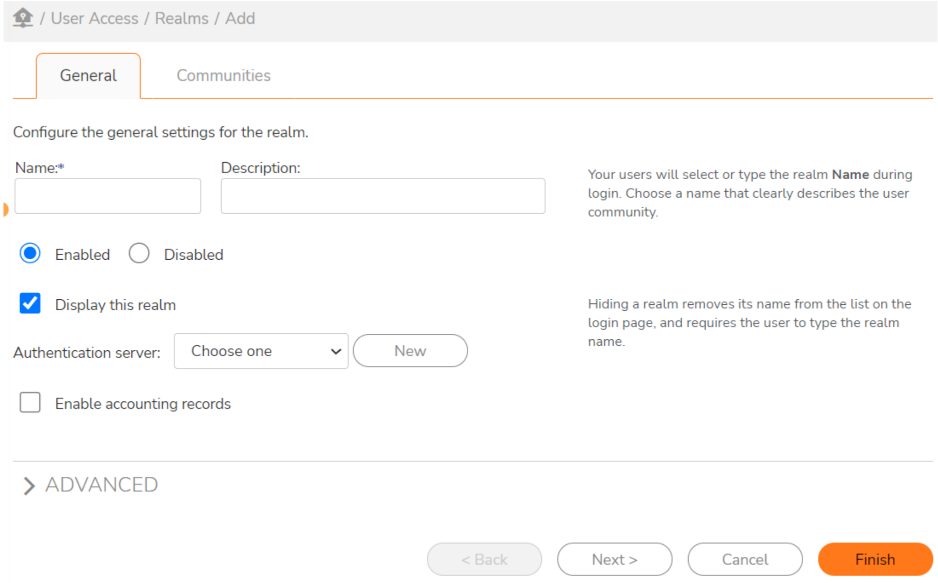
If you create more than one realms, then one realm is assigned as default. If needed you change the other realm as default realm.

After you create a realm and associate it with an external authentication server, you can either add one or more communities to the realm or use the preconfigured Default community. If you create and save a realm without assigning a community to it, AMC automatically assigns the Default community to the realm. See Using the Default Community and also Adding, Editing, Copying, and Deleting Objects in AMC.

To create a realm:

1. In the AMC, navigate to **User Access > Realms**.
2. Click **+ New realm**.

The **Configure Realm** page displays with the **General** settings displayed.



/ User Access / Realms / Add

General | Communities

Configure the general settings for the realm.

Name:* ____ Description: ____

Your users will select or type the realm **Name** during login. Choose a name that clearly describes the user community.

● Enabled ○ Disabled

☑ Display this realm

Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

Authentication server: Choose one [New]

□ Enable accounting records

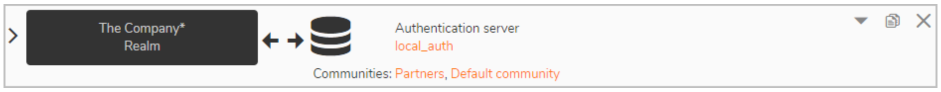
> ADVANCED

[< Back] [Next >] [Cancel] [Finish]

3. In the **Name** field, type a meaningful name for the realm. If users are required to select a realm name when logging in to the VPN, make sure the name clearly describes the user population.

4. In the **Description** field, type a descriptive comment about the realm. This is optional, but helpful, especially if your VPN uses multiple authentication realms.

   The text you enter in this field is displayed in the list of realms.



The Company* Realm

Authentication server
local_auth

Communities: Partners, Default community

5. Enable or disable this realm by selecting the appropriate **Status**.

   See Enabling and Disabling Realms for more information.

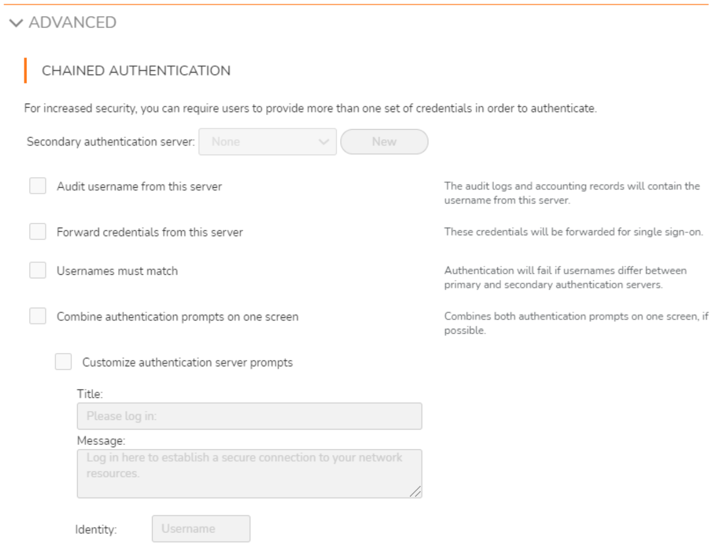
6. If you want this realm to appear in the list seen by your users (recommended in most cases), select the **Display this realm** checkbox.

7. From the **Authentication server** drop-down menu, select the Authentication Server used to verify a user’s identity. You must select a server.

8. You can also click **New** to display the **Authentication Servers > New Authentication Server** page for configuring a new authentication server and referencing it in the realm. For more information, see Configuring Authentication Servers.

9. If you want to save accounting information about this realm, select the **Enable accounting records** checkbox. When selected, all RADIUS, syslog, and routing changes are saved.

10. Click **Advanced** to display the advanced settings.



ADVANCED

CHAINED AUTHENTICATION

For increased security, you can require users to provide more than one set of credentials in order to authenticate.

Secondary authentication server: None New

□ Audit username from this server — The audit logs and accounting records will contain the username from this server.

□ Forward credentials from this server — These credentials will be forwarded for single sign-on.

□ Usernames must match — Authentication will fail if usernames differ between primary and secondary authentication servers.

□ Combine authentication prompts on one screen — Combines both authentication prompts on one screen, if possible.

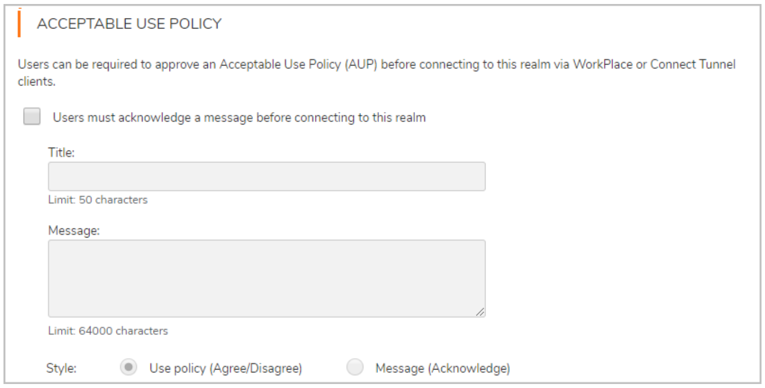
□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username

11. Set up the appliance to use a second authentication server and create a customized Acceptable Use Policy (AUP). There are two ways to set up a second authentication server:
    - **Chained authentication**: Require users to provide more than one set of credentials. See Configuring Chained Authentication.
    - **Enable group affinity checking**: Query a secondary authentication repository. See Enabling Group Affinity Checking in a Realm for more information.
12. In the **Acceptable Use Policy** area, select the **Users must acknowledge a message before connecting to this realm** checkbox to force users to agree to an Acceptable Use Policy before being allowed to log in to the realm.



ACCEPTABLE USE POLICY

Users can be required to approve an Acceptable Use Policy (AUP) before connecting to this realm via WorkPlace or Connect Tunnel clients.

□ Users must acknowledge a message before connecting to this realm

Title:

Limit: 50 characters

Message:

Limit: 64000 characters

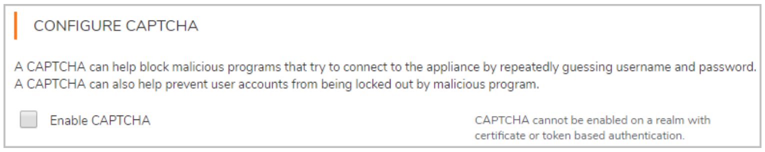
Style: ● Use policy (Agree/Disagree) ○ Message (Acknowledge)

13. In the **Title** field, type in the title of the AUP, up to 50 characters.
14. In the **Message** field, type in the AUP message to which the user needs to agree, up to 64,000 characters.
15. For the **Style** setting, select one of these radio buttons:
    - **Use policy (Agree/Disagree)** – The use policy agreement is displayed, and the user must click the **Agree** button to continue connecting. If **Disagree** is clicked, the session is ended.

- **Message (Acknowledge)** – The message is displayed, and the user clicks the **OK** button to continue connecting.

16. In the **Configure CAPTCHA** area, check the **Enable CAPTCHA** checkbox to require WorkPlace users to enter CAPTCHA characters in addition to a user name and password during login.

    The CAPTCHA prompt is displayed on the WorkPlace login page only if CAPTCHA is enabled here.

    CONFIGURE CAPTCHA

    A CAPTCHA can help block malicious programs that try to connect to the appliance by repeatedly guessing username and password. A CAPTCHA can also help prevent user accounts from being locked out by malicious program.

    □ Enable CAPTCHA

    CAPTCHA cannot be enabled on a realm with certificate or token based authentication.

    CAPTCHAs are effective in preventing these types of malicious program attacks on password systems:

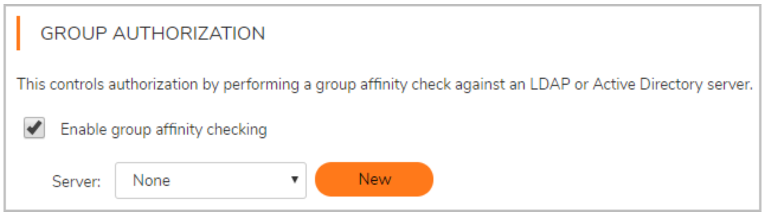
    - A bot that attempts to login by guessing the username/password by iterating through a dictionary of password possibilities.
    - A denial-of-service attack from a bot that attempts to lock out user accounts by forcing a sequence of numerous unsuccessful logins.

    A CAPTCHA is configured at the realm level across all WorkPlace access methods and all authentication service configurations (local Auth, LDAP, Active Directory, RADIUS). The CAPTCHA consists of 6 alphanumeric characters that are not case sensitive.

    Remember the following when using CAPTCHA:

    - In chained authentication mode, CAPTCHA is shown only for the primary authentication
    - CAPTCHA cannot be enabled on a Realm with token-based or certificate-based authentication. The CAPTCHA configuration section is disabled in these cases.

17. In the **Group authorization** area, check the **Enable group affinity checking** checkbox and select the server from the **Server** drop-down menu to perform a group affinity check against an LDAP or Active Directory server.

    GROUP AUTHORIZATION

    This controls authorization by performing a group affinity check against an LDAP or Active Directory server.

    ☑ Enable group affinity checking

    Server: None

    To add a new authentication server, click the **New** button to configure a new server as explained in Configuring Authentication Servers.

18. Click **Save**.

    You can add user communities to the realm (see Adding Communities to a Realm). If you create and save a realm without assigning a community to it, AMC automatically assigns the global Default community to the realm. For more information, see Using the Default Community.

    ⓘ **NOTE:** For information on how to edit, copy, and delete communities, see Adding, Editing, Copying, and Deleting Objects in AMC.

Adding Communities to a Realm

After you create a realm, the next step is to configure one or more communities that belong to it. If all users in a realm should be treated the same, then only a single community needs to be defined. Create additional communities if you want to subdivide users; you might want to give remote employees, for example, access methods and End Point Control restrictions that differ from those for local employees. Each community defines the following:

- A subset of users within a realm
- Which access methods are available to those users when they log in to a realm
- What restrictions (if any) are placed on their end point devices

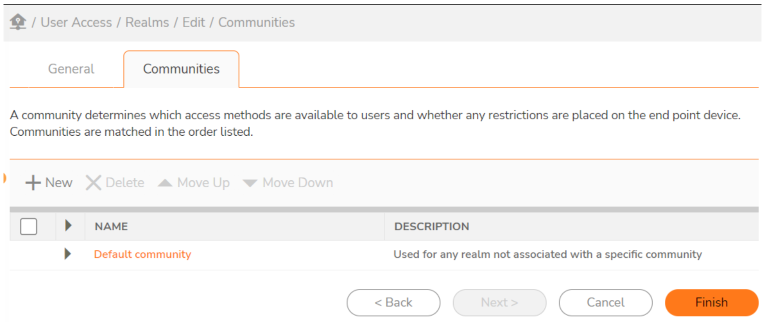
Each realm on the appliance must reference at least one community. Using multiple communities can be an efficient way of segmenting your user population to provide specific access agents to certain users or to place End Point Control restrictions on certain types of devices used by community members.

You can either use the preconfigured Default community (see Using the Default Community) or add other communities to the realm. As your user access or security policy requirements change over time, you can add additional communities to a realm, modify the user communities or delete them.

To add a community to a realm:

1. After creating a realm on the **General** tab of the **Configure Realm** page, go to the **Communities** page by clicking the **Next** button.

   The **Configure Realm page** displays with the **Communities** tab highlighted.

   A community determines which access methods are available to users and whether any restrictions are placed on the end point device. Communities are matched in the order listed.

NAME	DESCRIPTION
Default community	Used for any realm not associated with a specific community

2. Use the **Move Up** or **Move Down** links to move the selected community up or down to view the communities listed in the order you want.
3. To:
   - Create a new community for the realm, click the + (New) icon.
   - Edit an existing community, click its link.

     The **Configure Community** page displays. Follow the steps described in Creating and Configuring Communities.

Creating and Configuring Communities

Creating a community involves these basic steps:

- Assign members to the community
- Configure the tunnel setting required for network tunnel client and On Demand Tunnel agent
- Select browser access methods for the community
- Optionally, specify End Point Control restrictions for the community
- Specify a style and layout for the WorkPlace portal

Topics:

- Assigning Members to a Community
- Selecting Tunnel Access Methods for a Community
- Selecting Browser Access Methods for a Community
- Using End Point Control Restrictions in a Community
- Configuring the Appearance of WorkPlace

Assigning Members to a Community

The first step in creating a community involves specifying which users will be members. By default, a community is configured to include all users from the authentication realm to which it is assigned. However, you can configure a community to permit access to only a subset of users or user groups in a realm.

This is useful, for example, if you want to segment a realm into one community for employees and another community for business partners. You can then provide each community with the appropriate access agents or impose End Point Control restrictions if users are logging in from non-secure computers. Communities can also be referenced in access control rules to permit or deny access to your resources.

To assign members to an existing community:

1. From the main navigation menu, click **Realms**.
2. Within the realm, click the link for the community you want to configure.

   The **Configure Community** page displays with the **Members** tab displayed.
3. The **Members** menu specifies which users or groups belong to this community. Click **Edit** to select from a list of users and groups. If no users or groups are specified, the default value of this field is **Any**, meaning that any users from the authentication realm that references this community belong to this community.
4. In the **Maximum active sessions** field you can limit the number of sessions each member of this community is allowed to have active at one time. For mobile users, for example, you may want to restrict the number of sessions to 1—each session consumes one user license, and it’s impractical for a mobile user to have more than one active session. With other communities, such as employees who alternate between working from home and in the office, the number of allowed sessions should probably be higher. See How Licenses Are Calculated for more information.

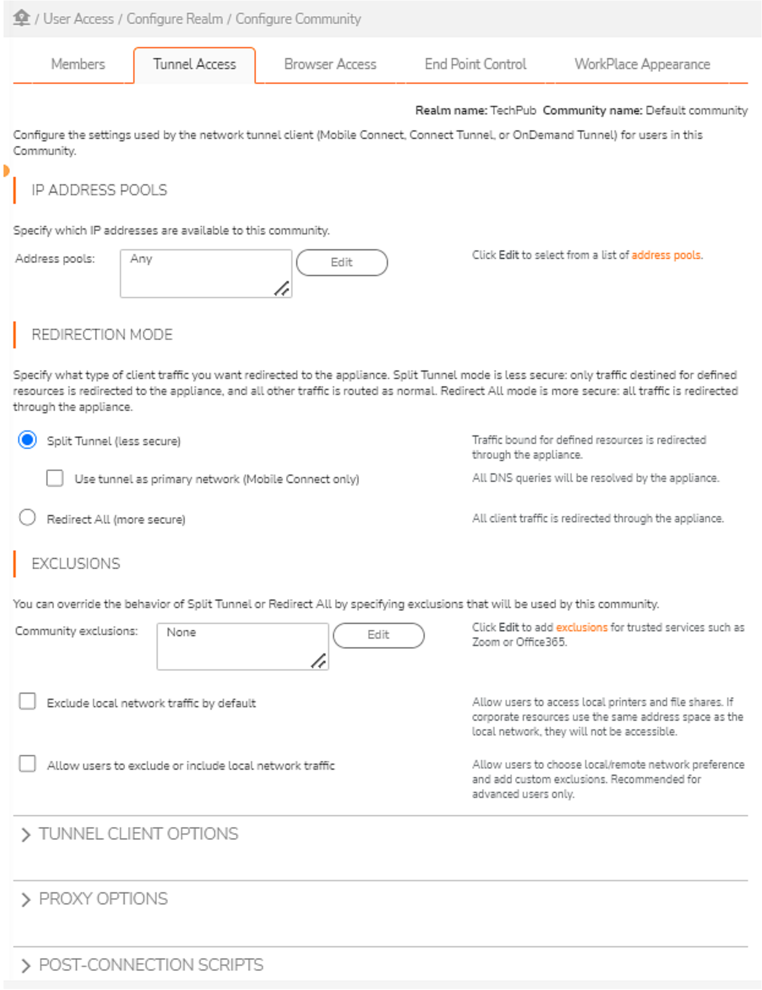
5. To select which access methods are available to members of the community, click the **Access Methods** tab. See Selecting Tunnel Access Methods for a Community for more information.
6. To restrict user access based on the security of client devices, click the **End Point Control restrictions** tab and specify which zones are available to users in this community. See Using End Point Control Restrictions in a Community.
7. Click **Save**.

Selecting Tunnel Access Methods for a Community

The second step in creating a community is to determine which tunnel access methods will be available for community members to connect to the appliance and access your network resources. For information on which access methods are compatible with your users' environments, see User Access Components. In this page, you can configure the settings used by the network tunnel client (Mobile Connect, Connect Tunnel, or OnDemand Tunnel) for users in a Community.

To specify the tunnel access methods available to community members:

1. In the AMC, navigate to **User Access > Realms**.
2. Click the link for the community you want to configure.
3. Click the **Tunnel Access** tab.



/ User Access / Configure Realm / Configure Community

Realm name: TechPub **Community name:** Default community

Configure the settings used by the network tunnel client (Mobile Connect, Connect Tunnel, or OnDemand Tunnel) for users in this Community.

IP ADDRESS POOLS

Specify which IP addresses are available to this community.

Address pools: Any

Click **Edit** to select from a list of address pools.

REDIRECTION MODE

Specify what type of client traffic you want redirected to the appliance. Split Tunnel mode is less secure: only traffic destined for defined resources is redirected to the appliance, and all other traffic is routed as normal. Redirect All mode is more secure: all traffic is redirected through the appliance.

● Split Tunnel (less secure) — Traffic bound for defined resources is redirected through the appliance.

□ Use tunnel as primary network (Mobile Connect only) — All DNS queries will be resolved by the appliance.

○ Redirect All (more secure) — All client traffic is redirected through the appliance.

EXCLUSIONS

You can override the behavior of Split Tunnel or Redirect All by specifying exclusions that will be used by this community.

Community exclusions: None

Click **Edit** to add exclusions for trusted services such as Zoom or Office365.

□ Exclude local network traffic by default — Allow users to access local printers and file shares. If corporate resources use the same address space as the local network, they will not be accessible.

□ Allow users to exclude or include local network traffic — Allow users to choose local/remote network preference and add custom exclusions. Recommended for advanced users only.

4. By default, any configured IP address pool is available to the selected community. To select specific IP address pools, click **Edit** in the IP address pools area and then select from the list of configured pools.
5. Select the Redirection mode used to route client traffic to the appliance. The network tunnel service supports several redirection modes. For a more detailed description of the supported redirection modes, see Redirection Modes.
    - Split Tunnel (less secure): Traffic bound for resources defined in AMC is redirected through the tunnel, and all other traffic is routed as normal.
        - Enable **Use tunnel as primary network (Mobile Connect only)** checkbox. The appliance will resolve all the DNS queries when you enable the checkbox.
    - Redirect All (more secure): Traffic is redirected through the tunnel regardless of how resources are defined in AMC.
6. You can override the behavior of Split Tunnel or Redirect All by specifying exclusions that will be used by this community.

   In the **Community Exclusions** field, enter the host names, IP addresses, subnets, and IP ranges that you want to exclude from being redirected through the appliance. Wildcard characters (* and ?) are permitted.

ⓘ | **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

For example, if you have three public web servers (www.YourCompany.com, www2.YourCompany.com, and www3.YourCompany.com), you can allow the network traffic associated with them to avoid the appliance, which will improveperformance. Add all three public sites to the Exclusions by using a wildcard character: www?.YourCompany.com. Resources in this list can also contain variables.

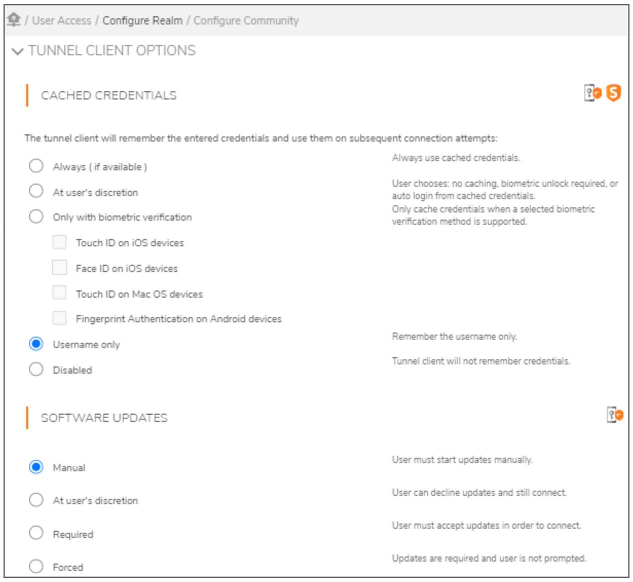
ⓘ | **NOTE:** You should define the corresponding IP/Range/Subnet in Wildcard exclusion.

Enable **Exclude local network traffic by default** checkbox if you want to allow users to access local printers and file shares. If corporate resources use the same address space as the local network, they will not be accessible.

Enable **Allow users to exclude or include local network traffic** if you want to allow users to choose local/remote network preference and add custom exclusions. Recommended for advanced users only.

Configuring Tunnel Client Options, Proxy Options, Post-Connection Strips, and Advanced information

1. (Optional) Click to expand the **Tunnel Client Options** section:



/ User Access / Configure Realm / Configure Community

TUNNEL CLIENT OPTIONS

CACHED CREDENTIALS

The tunnel client will remember the entered credentials and use them on subsequent connection attempts:

○ Always (if available)	Always use cached credentials.
○ At user's discretion	User chooses: no caching, biometric unlock required, or auto login from cached credentials.
○ Only with biometric verification	Only cache credentials when a selected biometric verification method is supported.
□ Touch ID on iOS devices	
□ Face ID on iOS devices	
□ Touch ID on Mac OS devices	
□ Fingerprint Authentication on Android devices	
● Username only	Remember the username only.
○ Disabled	Tunnel client will not remember credentials.

SOFTWARE UPDATES

● Manual	User must start updates manually.
○ At user's discretion	User can decline updates and still connect.
○ Required	User must accept updates in order to connect.
○ Forced	Updates are required and user is not prompted.

- In the **Caption for start menu and icon** field, type the customized text that you want to appear for the Connect Tunnel client on the menu and beneath the Connect icon on the user's desktop.
- **Create icon on desktop**: Places the Connect Tunnel client icon on the desktop.
- **Run at system startup**: Automatically runs the Connect Tunnel client when the operating system starts on the user's computer (Windows only).

2. Scroll down to the **Cached Credentials** section and select one of these options:

Option	Description
Always (if available)	Always use cached credentials
At user's discretion	Choose no caching, biometric unlock required, or auto login from cache.
Only with biometric verification	Only use credential caching when biometric verification is supported and enabled. Cached credentials are only used after biometric identification verification.
Username only	Use cached username.
Disabled	Disable cached credentials in the Connect Tunnel client.

ⓘ **NOTE:** On a Windows system, Connect Tunnel uses cached system credentials. On other systems, Connect Tunnel remembers the entered credentials and uses them on subsequent connection attempts.

3. Use one of the **Software updates** options to alert users when client updates are available or update their software automatically. This setting is available only when the network tunnel client is configured to provision client from Secure Mobile Access WorkPlace:

Option	Description
Manual	User must start updates manually.
At user's discretion	Allows users to decide when to install software updates. The update can be deferred indefinitely; however, the user will see the software-update alert when he or she starts the tunnel client (once per day) until the update is installed.
Required	User must accept updates in order to access VPN resources through the tunnel client.
Forced	Updates are required in order to connect. The update program starts, and a progress bar is visible during installation, but the user is not prompted during the process.

4. To automatically establish a tunnel connection when a user attempts to login from an unsecure location, check the **Enable secure network detection** check box in the **Secure Network Detection** section. For more information, see Secure Network Detection.

5. By default, the client is configured to access the realm and appliance name from which the client was downloaded. However, you can override this default behavior and configure the client to access a different realm or appliance. In the **Custom connection** area, select the **Configure client with custom realm and appliance FQDN** check box, and then specify these options as needed:

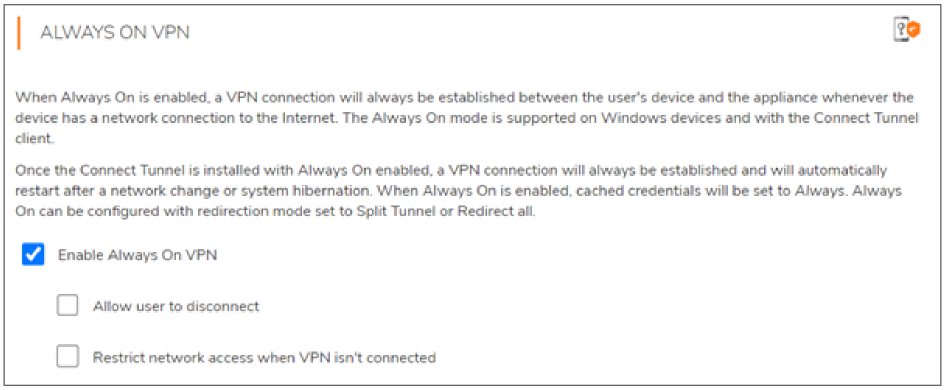
   - From the **Realm name** list, click the name of the default realm.
   - In the **Appliance FQDN** field, type the fully qualified domain name of the default appliance.

6. By default, a tunnel client session is never terminated by the appliance once it has been established: users can leave sessions idle and return to them later without having to reauthenticate. If you want to require users to re-authenticate after a certain period of time, in the **Session Termination** section, select **Limit session length to credential lifetime**. This requires users to re-authenticate once the amount of time specified by **Credential lifetime** (on the **Configure General Appliance Options** page) has passed. When this option is selected, users are notified when a session is nearing the inactivity threshold and users can avert the disconnect by performing any mouse or keyboard activity.

   If you need a TCP connection or consistent UDP traffic flow between the same two address/port tuples to live longer than eight hours, you must put the user in a community that has this option unchecked. Even with the **Limit session length to credential lifetime** check box unchecked, users cannot authorize new flows within the tunnel after their credentials expire.

7. Scroll down to **Always On VPN** section and check the **Enable Always On VPN** box.

   Selecting **Enable Always On VPN** option establishes a VPN connection between the user's device and the appliance whenever the device has a network connection to the internet.



ALWAYS ON VPN

When Always On is enabled, a VPN connection will always be established between the user's device and the appliance whenever the device has a network connection to the Internet. The Always On mode is supported on Windows devices and with the Connect Tunnel client.

Once the Connect Tunnel is installed with Always On enabled, a VPN connection will always be established and will automatically restart after a network change or system hibernation. When Always On is enabled, cached credentials will be set to Always. Always On can be configured with redirection mode set to Split Tunnel or Redirect all.

☑ Enable Always On VPN

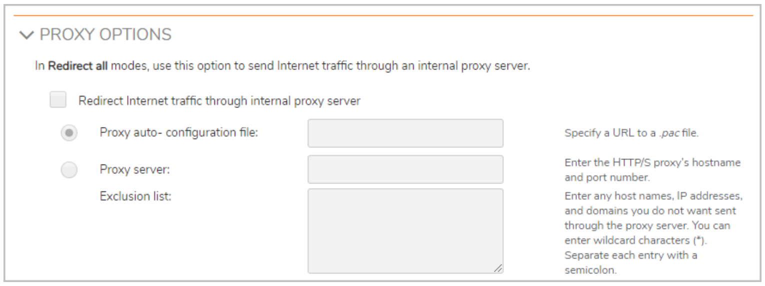
□ Allow user to disconnect

□ Restrict network access when VPN isn't connected

Option	Description
Allow user to disconnect	To allow users to unlock the Connect Tunnel client, disconnect the VPN connection, and modify the Always On VPN profile.
Restrict network access when VPN is not Connected	To restrict network access to the users until VPN is completely connected.

ⓘ | **NOTE:** Always On VPN is only supported for Connect Tunnel for Windows in SMA 12.4.

8. If you enabled **Redirect all** in the **Redirection mode** area, you can configure Internet traffic to be sent through an internal proxy server when the VPN connection is active. In the **Proxy options** area, select the **Redirect Internet traffic through internal proxy server** checkbox, and then select one of the proxy server options.



PROXY OPTIONS

In **Redirect all** modes, use this option to send Internet traffic through an internal proxy server.

□ Redirect Internet traffic through internal proxy server

● Proxy auto- configuration file: — Specify a URL to a *.pac* file.

○ Proxy server: — Enter the HTTP/S proxy's hostname and port number.

Exclusion list: — Enter any host names, IP addresses, and domains you do not want sent through the proxy server. You can enter wildcard characters (*). Separate each entry with a semicolon.

To specify a proxy auto-configuration (`.pac`) file, click **Proxy auto-configuration file** and then type the URL, preceded by the `http://` protocol identifier, for the `.pac` file. The `.pac` file configures the user's Web browser to load its proxy configuration settings from a JavaScript file rather than from information that you manually specify; the JavaScript file specifies which proxy servers can be used and can redirect specific URLs to specific proxy servers. For information about formatting `.pac` files, see:

http://en.wikipedia.org/wiki/Proxy_auto-confighttp://en.wikipedia.org/wiki/Proxy_auto-config

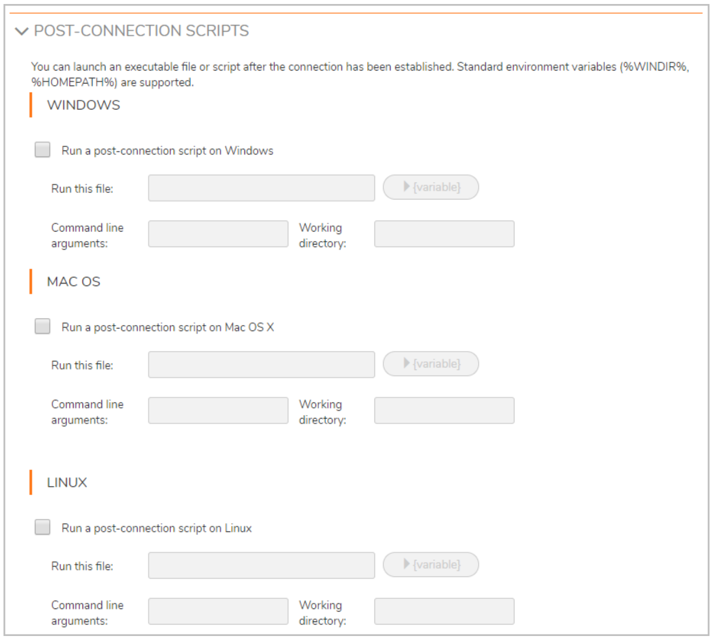
To manually specify a proxy server, click **Proxy server** and then type the server's host name and port number in `host:port` format (for example, `myhost:80`). Optionally, in the **Exclusion list** field, you can type the host names, IP addresses, or domain names of any resources that you do not want redirected through the proxy server. When defining these resources, wild cards are valid, and multiple entries must be separated by semicolons.

9. To launch an executable file or script after the connection has been established:

a. Click to expand the **Post-connection scripts** area.

b. Select the **Run a post-connection script** checkbox that corresponds to your operating system.

c. Specify your settings. For more information, see Post-Connection Scripting.



POST-CONNECTION SCRIPTS

You can launch an executable file or script after the connection has been established. Standard environment variables (%WINDIR%, %HOMEPATH%) are supported.

WINDOWS

□ Run a post-connection script on Windows

Run this file: {variable}

Command line arguments: Working directory:

MAC OS

□ Run a post-connection script on Mac OS X

Run this file: {variable}

Command line arguments: Working directory:

LINUX

□ Run a post-connection script on Linux

Run this file: {variable}

Command line arguments: Working directory:

1. In the **Run this file** field, type the path and name for the script file. For example:

   `%Program Files%\ACME\remote_access.bat`

2. (Optional) In the **Command line arguments** field, type any command-line arguments that you want to execute when running the script. For example:

   `-user=%USERNAME% -system=%OS%`

3. (Optional) In the **Working directory** field, type the directory in which the script will be executed. When defining the working directory, you can specify environment variables formatted as `%VariableName%`, where `VariableName` represents the actual environment variable name. For example:

   `%USERPROFILE%\ACME`

ⓘ **NOTE:** The post connection script file must be in a location on the client computer that the user can access and where that user can execute files.

10. In the **Advanced** area, **Enable ESP encapsulation of tunnel network traffic** is selected by default for all network traffic (for all tunnel traffic). ESP (Encapsulating Security Payload) is a way to encapsulate and decapsulate packets inside of UDP packets for traversing Network Address Translators (NATs). Using it can improve the performance of applications, especially UDP-streaming applications like VoIP.

    For an ESP tunnel to function, UDP port 4500 needs to be open in the firewall for traffic to and from the SMA appliance external IP and Virtual IP addresses.

    When ESP is enabled, the tunnel client tries to bring up an ESP tunnel, but falls back to a legacy SSL tunnel if there is a problem establishing the ESP tunnel. The typical reason for this failure is that UDP port 4500 is not open in the network firewall.

If you do not want to use ESP because you do not want to open UDP port 4500 in your firewall or for any reason, then clear the **Enable ESP encapsulation of tunnel network traffic** checkbox. To disable the default use of ESP in a community, clear the checkbox on the **Realms > [*your tunnel realm*] > Communities > [*your tunnel community*] > Access Methods > Tunnel Access > Advanced**.

11. Click **OK**.

ⓘ | **NOTE:**

- If users are running OnDemand Tunnel in “redirect all” mode, connections to translated Web resources fail with `Page cannot be displayed` errors. To work around this issue, add an A (Address) record to the internal DNS servers to assign the appliance VIP or external IP to the appliance FQDN.
- When **At user’s discretion** is enabled for **Client software updates** in the **Software updates** area, the user sees an upgrade notification, and the Connect Tunnel client caches the user’s response for 24 hours. If the setting is then changed to **Required** or **Forced**, a user who opted to delay updating may not be prompted again until the following day because the earlier response is still cached.
- If you plan to run a VB script after a connection has been established, you cannot simply enter the path and name of the `.vbs` script file; you must use the Windows Script Host utility to invoke it. To work around this, configure the post-connection options as follows:
  - **Run this file**: `<drive>:\windows\system32\cscript.exe`
  - **Command line arguments**: `<Path to script>`. For example:

    `c:\path\to\script.vbs or \\path\to\script.vbs`

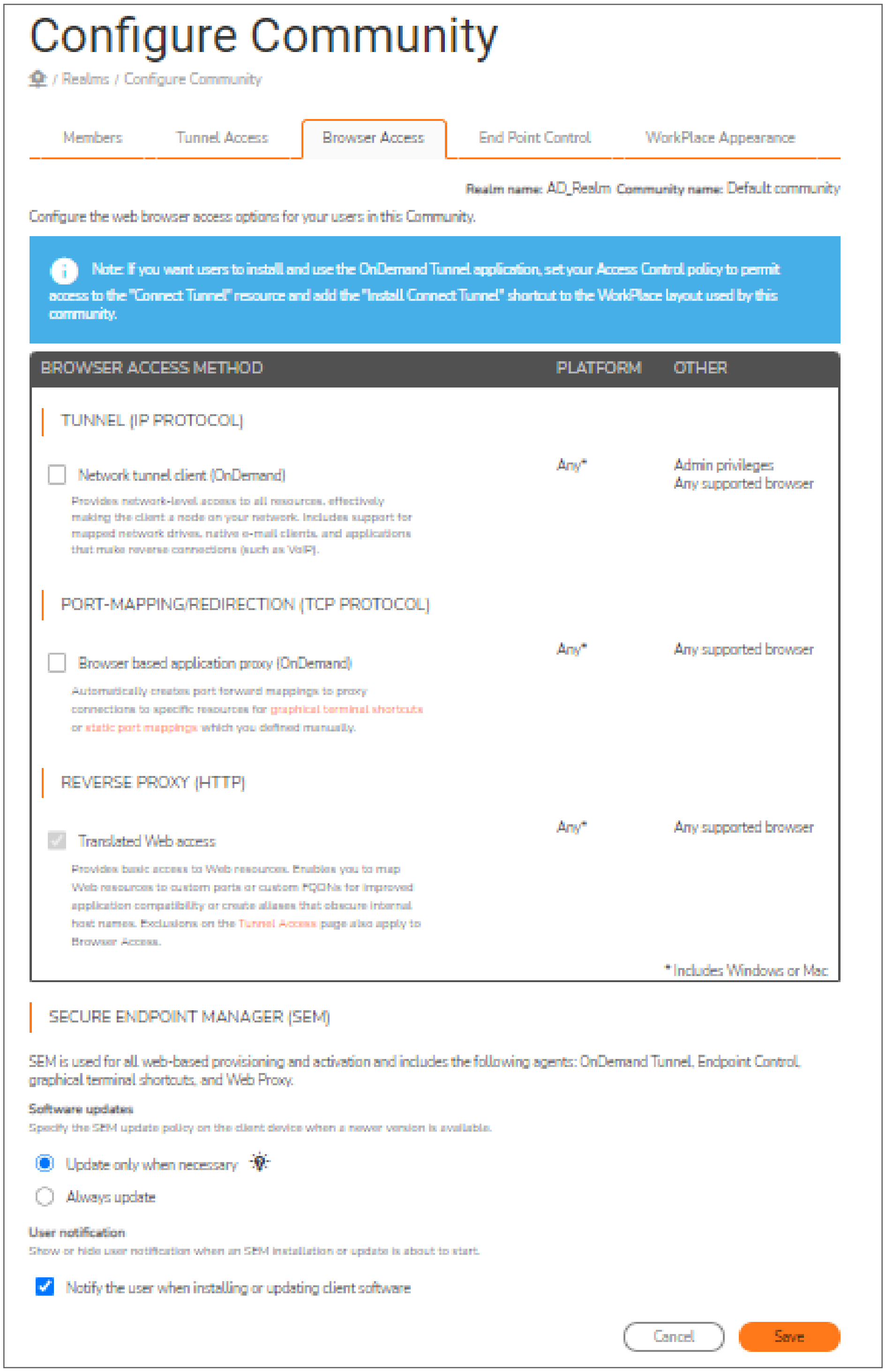
  Leave **Working directory** empty.
- When you specify a `.pac` file location, be certain that your tunnel users have access to it. You can do this by defining a resource and creating an access rule. See Creating and Managing Resource Groups and Configuring Access Control Rules.

Selecting Browser Access Methods for a Community

The third step in creating a community is to determine which browser access methods will be available for community members to connect to the appliance and access your network resources. For information on which access methods are compatible with your users’ environments, see User Access Components.

To specify the browser access methods available to community members:

1. In the AMC, navigate to **User Access > Realms**.
2. Click the link for the community you want to configure.
3. Click the **Browser Access** tab.



Configure Community

/ Realms / Configure Community

Realm name: AD_Realm **Community name:** Default community

Configure the web browser access options for your users in this Community.

Note: If you want users to install and use the OnDemand Tunnel application, set your Access Control policy to permit access to the "Connect Tunnel" resource and add the "Install Connect Tunnel" shortcut to the WorkPlace layout used by this community.

BROWSER ACCESS METHOD	PLATFORM	OTHER
TUNNEL (IP PROTOCOL)		
□ Network tunnel client (OnDemand) Provides network-level access to all resources, effectively making the client a node on your network. Includes support for mapped network drives, native e-mail clients, and applications that make reverse connections (such as VoIP).	Any*	Admin privileges Any supported browser
PORT-MAPPING/REDIRECTION (TCP PROTOCOL)		
□ Browser based application proxy (OnDemand) Automatically creates port forward mappings to proxy connections to specific resources for graphical terminal shortcuts or static port mappings which you defined manually.	Any*	Any supported browser
REVERSE PROXY (HTTP)		
☑ Translated Web access Provides basic access to Web resources. Enables you to map Web resources to custom ports or custom FQDNs for improved application compatibility or create aliases that obscure internal host names. Exclusions on the Tunnel Access page also apply to Browser Access.	Any*	Any supported browser

* Includes Windows or Mac

SECURE ENDPOINT MANAGER (SEM)

SEM is used for all web-based provisioning and activation and includes the following agents: OnDemand Tunnel, Endpoint Control, graphical terminal shortcuts, and Web Proxy.

Software updates

Specify the SEM update policy on the client device when a newer version is available.

● Update only when necessary

○ Always update

User notification

Show or hide user notification when an SEM installation or update is about to start.

☑ Notify the user when installing or updating client software

4. Select the access methods community members can use with a browser to connect to resources on your network. Based on the capabilities of the user's system, the appliance activates the access agents you

have selected. For information on the capabilities and system requirements of the various access agents, see User Access Components and Services.

5. If you want to provide network tunnel client access to members of a community, select a combination of the following:
   - In the **Tunnel (IP Protocol)** section, select **Network tunnel client (OnDemand)**. You can use a built-in resource and shortcut if you want users to download the Connect Tunnel client and activate it from a link in WorkPlace.
   - For Web-based proxy access, in the **Port-Mapping/Redirection (TCP Protocol)** section, select **Browser based application proxy (OnDemand)**.
   - In the **Reverse Proxy (HTTP)** section, **Translated Web access** is always selected. This provides clientless access to Web resources that are mapped to custom ports or custom FQDNs for improved application compatibility or that use aliases to obscure internal host names. See Web Access for information about the different types of Web access, and see Adding Resources for information about adding Web-based resources.
6. Select the required option to specify the SEM update policy on the client device when a newer version is available and enable **Notify the user when installing or updating client software** checkbox if you to show or hide user notification when an SEM installation or update is about to start.
7. Click **Save**.

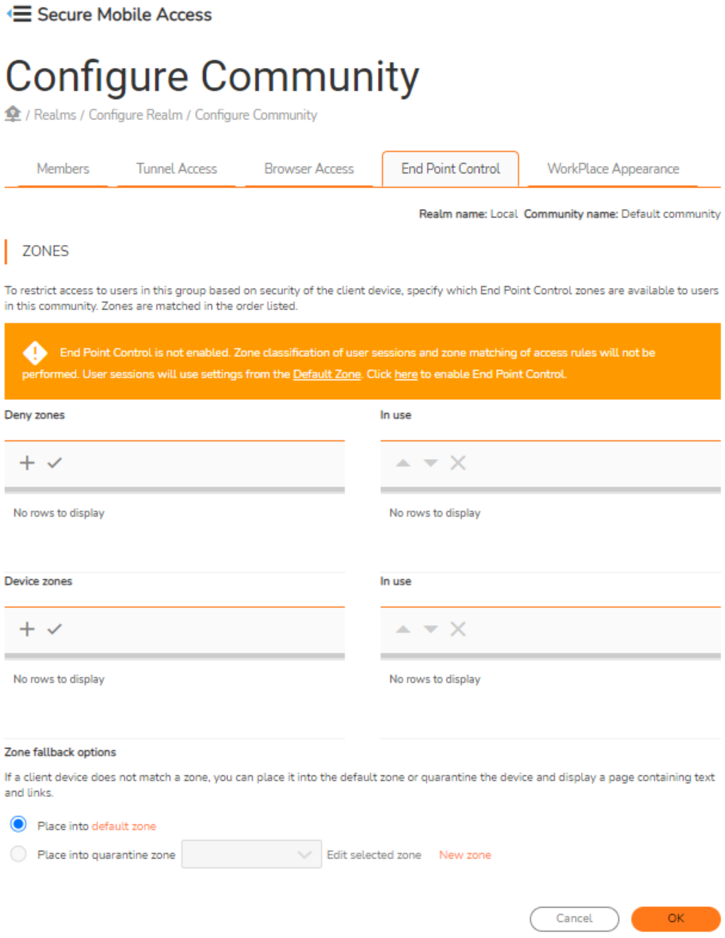
Using End Point Control Restrictions in a Community

When you're creating a community, you have the option of restricting access to users based on the security of their client devices. To do this, specify which End Point Control zones are available to users in this community. There are four types of zones—Deny, Device, Quarantine, and Default. For more information on how to create and configure End Point Control zones, and the device profiles they use to classify connection requests, see Managing EPC with Zones and Device Profiles.

You can also set an inactivity timer, even if you don't use End Point Control zones for a community, if your users access the appliance using the Connect Tunnel client.

To apply End Point Control restrictions for a community:

1. In the AMC, navigate to **User Access > Realms**.
2. Click the link for the community you want to configure, and then click the **End Point Control** tab.



Secure Mobile Access

Configure Community

/ Realms / Configure Realm / Configure Community

Realm name: Local **Community name:** Default community

ZONES

To restrict access to users in this group based on security of the client device, specify which End Point Control zones are available to users in this community. Zones are matched in the order listed.

End Point Control is not enabled. Zone classification of user sessions and zone matching of access rules will not be performed. User sessions will use settings from the Default Zone. Click here to enable End Point Control.

Deny zones	In use
No rows to display	No rows to display

Device zones	In use
No rows to display	No rows to display

Zone fallback options

If a client device does not match a zone, you can place it into the default zone or quarantine the device and display a page containing text and links.

● Place into default zone

○ Place into quarantine zone Edit selected zone New zone

3. Use a Deny zone if you have a device profile that is unacceptable in your deployment. You might, for example, want to deny access to any user who has Google Desktop installed on the PC with which they are trying to connect. Select (or create) an entry in the **Deny zones** list and click the **>>** button to move it to the **In use** list. Deny zones are evaluated first (if there's a match, the user is logged off).

   To create a new EPC zone and then add it to the list, click the **+ (New)** icon. For information on how to create a zone, see Defining Zones.

4. You can assign one or more End Point Control Device zones to the community, which are used to determine which devices are authorized to access a community. If you don't select a zone, community members are assigned to the default zone, which could limit or even deny access to resources, depending on your access policy. Select the checkbox for a zone in the **Device zones** list and then click the checkmark (✓) at the top of the list to add it to the **In Use** list.

5. If the community references more than one zone, use **Move Up** and **Move Down** to arrange their order in the list. Zones are matched in the order they are listed, so it is important to you consider which devices are authorized in each zone. You should place your most specific zones at the top of the list.

6. If a client device does not match a zone, use the settings in the **Zone fallback options** area to place it into the default zone, or quarantine the device and (optionally) display a customized page with text and links. See Creating a Quarantine Zone for more information.
7. To set the Inactivity Timer (which is triggered when there is no keyboard or mouse activity) for community members, select a time limit (ranging from **After 3 mins** to **After 24 hours** or **Never**) from the **End inactive user connections** list. This is a Windows-only setting that is used by the network tunnel client.

   ⓘ **NOTE:** If End Point Control is not used in a community, or at all, the Inactivity Timer is still effective for user sessions, as the Default Zone will still be applied.
8. Click **Save** to complete the configuration of the community.

   ⓘ **NOTE:** The appliance uses EPC interrogation to check for certain device profile attributes on the client and then classifies the device accordingly. If a Quarantine zone is your fallback option, and if EPC interrogation somehow fails, a device that would normally be quarantined may instead end up in the Default zone.

Configuring the Appearance of WorkPlace

Each community can be assigned a style and layout for its WorkPlace portal content pages.

A WorkPlace style determines the colors, fonts, and images used to display the pages, and a layout determines page content, how it is arranged, and how you navigate the portal. Keep in mind that the style for the login, error, and notification pages is specified when you set up a site.

To create a style and layout for a community:

1. In the AMC, navigate to **User Access > Realms**.
2. Click the link for the community you want to configure, and then click the **WorkPlace Appearance** tab.
3. Select an existing style or click **Manage styles** to modify or create one.

   For more information on configuring a WorkPlace style, see Creating or Editing a WorkPlace Style.
4. Select an existing layout or click **Manage layouts** to modify or create one.

   For more information on configuring a WorkPlace layout, see Creating or Editing a WorkPlace Layout.
5. The layout for this community is changed automatically to accommodate smaller devices; for example, the **Intranet Address** field (if it is part of the layout) is displayed on an advanced mobile device, but not a basic one.

   If that result is not acceptable, you can specify a different layout for different classes of devices in the **Small form factor devices** area. A good approach when creating a community is to see how the WorkPlace portal for this community looks on a mobile device by default, and then create a new layout or modify an existing one only if you need to.

WorkPlace and Small Form Factor Devices

WorkPlace provides support for a variety of small form factor devices, including PDAs, Pocket PCs, smart phones, WAP 2.0-compatible phones, and i-mode phones. This section explains how to configure the appliance to support these devices.

Topics:

- About WorkPlace and Small Form Factor Devices
- Optimizing WorkPlace for Display on Small Form Factor Devices

About WorkPlace and Small Form Factor Devices

When a user logs in to WorkPlace from a small form factor device, WorkPlace detects the device type and automatically transforms to best match the capabilities of the client device. This transformation affects several aspects of the user experience:

- **WorkPlace functionality**: Some WorkPlace features available from a standard desktop browser are omitted on small form factor devices:
  - The **Network Explorer** page is not available for accessing network shares.
  - The **Intranet Address** box is not available for typing a URL or UNC path name.
- WorkPlace http and https bookmarks are supported.
- SonicWall access agents are not supported, including the OnDemand access agent, the EPC data protection agents, and terminal server agents.
- The custom online Help file is not available.
- **WorkPlace look and feel**: The standard WorkPlace appearance (including any customization you've made) is automatically modified for optimal display on small form factor devices.

  ⓘ | **NOTE:** For information about configuring the appearance of WorkPlace on a small form device, see Optimizing WorkPlace for Display on Small Form Factor Devices .
- **Resource availability**: You can control which WorkPlace shortcuts will appear on a small form factor device. This allows you to avoid Web resources that are incompatible with a particular type of device.

  For example, you might want to hide the link for Outlook Web Access and instead provide a link to Outlook Mobile Access. This setting is controlled when creating a WorkPlace shortcut; for more information, see Adding Web Shortcuts.
- **End Point Control classification**: To restrict access based on device type, you can create an EPC zone for a specific type of Android mobile device and then reference that zone in an access control rule. For more information, see Defining Zones.

The appliance is pre-configured to classify most common small form factor devices into one of several categories. The default settings should be sufficient for most deployments, but you can modify the configuration to change the classification or recognize other devices, as needed.

ⓘ | **NOTE:**

- Some small form factor devices do not display error pages, but instead return an error code (such as a `500` error) from the Web server, without any descriptive error text.
- Users attempting to log in to WorkPlace from an unsupported device will receive an error message.
- For users who connect to the appliance from small form factor devices, you should configure the appliance with a certificate from a leading CA (such as VeriSign), or else import the CA certificate to your

users' small form factor devices—many devices will fail to connect when presented with a certificate from an unknown CA and will not provide any error message. For more information, see CA Certificates.

Optimizing WorkPlace for Display on Small Form Factor Devices

The general WorkPlace appearance, including any customization you've made, is automatically modified for optimal display on small form factor devices. The results are sufficient for most deployments, but you may want to manually configure a few settings to improve the display. Most of the settings are configured as part of a WorkPlace *style*; when you configure a WorkPlace *layout* you'll be able to see how page navigation and other elements will work on different mobile devices.

To optimize a WorkPlace site for display on small form factor devices:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **Appearance** tab.
3. In the **Styles** section, choose an existing style to base your new one on (select its checkbox or click the **+** (New) icon.
4. In the **Images** area, specify a logo for WorkPlace. For optimum results on smaller devices, the image should not exceed 100 pixels by 40 pixels. By default, the logo specified in the **Standard logo image file** box is used. To specify an alternate image, type the path of the `.gif`, `.jpg`, or `.png` file in the **Replace with** field, or click **Browse** to locate it. Graphics are automatically omitted from WAP and i-mode devices: this setting does not affect the display on those devices.
5. To reduce the amount of vertical scrolling required, clear the **Display greeting on small form factor devices** checkbox in the **Text and Files** area.
6. Click **Save** or **Finish** to save your WorkPlace site settings, or click **Reset Defaults** to restore the factory default WorkPlace site settings.

ⓘ **NOTE:** If you are using a mobile device that doesn't support UTF-8, such as the Sanyo W32SA handset, localized content is displayed using illegible characters. To log in, the user must enter his or her credentials in ASCII format.

To preview a WorkPlace layout on a small form factor device:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **Appearance** tab.
3. In the **Layouts** drop-down list, select the layout you plan to use, or click the **+** (New) icon to configure one.
4. **General** settings: If your layout contains more than one page, you can specify the kind of navigation controls that will be displayed. Only an advanced mobile device, which is defined as one that has a browser that supports JavaScript, supports multiple pages.
5. **Device preview**: There are two approaches to lay out a community on smaller devices.
    - You can have the appliance accommodate smaller devices automatically. For example, the **Intranet Address** field (if it is part of the layout) is automatically not displayed on mobile devices, and whatever logo you have specified is scaled down.

- If the automatic results are not acceptable, you can create a different layout, intended only for mobile devices, and then specify it when you configure the community. See Configuring the Appearance of WorkPlace for more information.

Creating or Editing a WorkPlace Style

To create a new WorkPlace style:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **Appearance** tab.
3. In the **Styles** section, choose an existing style to base your new one on (select its checkbox, and then click **Copy** icon), or click the **+** (New) icon.
4. In the **Name** field, type a unique name for the WorkPlace style.
5. (Optional) In the **Description** field, type a descriptive comment about the style.
6. In the **Font family** list, select the type of font you want to use (**Serif** or **Sans-serif**).
7. In the **Color scheme** drop-down menu, click the name of the color scheme you want to use. If you select **Custom**, you can set custom colors for the WorkPlace **Page background**, **Subheadings**, and **Main heading**. Specify color settings by typing the applicable hexadecimal RGB value, or by clicking a color swatch and then selecting a color from the **Please choose a color**.
8. To replace the Secure Mobile Access logo that is displayed in WorkPlace with a different image, use the **Replace with** field to enter or browse for the `.gif` or `.jpg` file you want to use. For best results, the image should not exceed 200 pixels wide by 50 pixels high.
9. On small form factor devices, the logo specified in the **Images** area is resized by default, but for best results you may want to specify an alternate image that does not exceed 40 pixels by 100 pixels. Type the path of the image file, or click the **Browse** button to select the image file you want to use. The logo is automatically omitted from WAP and i-mode devices, so this setting does not affect the display on those devices.
10. In the **Title** field, type the text that will appear as the title on the page and in the browser’s title bar. The title must be no longer than 25 characters.
11. In the **Greeting** field, type the introductory text that should appear below the title. The greeting must not exceed 250 characters, but you may want to use a shorter one, especially if you want it to appear on small form factor devices.
12. To further assist the user, you could specify a custom **Help file** that provides more detailed information about the resources available on your VPN, or describe how to get technical support. Click **Browse** to specify a well-formed HTML file that contains custom Help information. Your custom Help content is integrated with the default WorkPlace Help system. To make changes to your custom help content, edit the file locally and upload it to the appliance again.
13. Click **Save** to save your WorkPlace site settings, or click **Reset Defaults** to restore the factory-default settings.

Creating or Editing a WorkPlace Layout

To create a new WorkPlace layout:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **Appearance** tab.
3. In the **Layouts** section, choose an existing style to base your new one on (select its checkbox, and then click **Copy** icon), or click the **+** (New) icon.
4. In the **Name** field, type a unique name for the WorkPlace layout.
5. (Optional) In the **Description** field, type a descriptive comment about the layout.
6. In the **Initial content** area, select a layout for your current WorkPlace content (any shortcuts and shortcut groups that you've defined), or choose to set up an initial structure for your content and add WorkPlace resources later. No matter how you decide to lay out your initial content, you can change it later by adding, removing, or rearranging pages and page content.
7. In the **Page navigation** area, specify the kind of navigation controls that will be displayed if your content requires more than one page.
8. Specify whether the **Intranet Address** field will be displayed when this layout is used. It gives users access to resources by typing a resource name (a UNC path, URL, or both). Click **Next**.
9. Click the **Edit page properties** link to change the basic properties of this WorkPlace page: its name (for example, *Home*) and a short description.
10. Use the page, column, and shortcut controls to add pages, content, and rearrange the elements on each page. Rearranging items in a layout or deleting them from a layout does not affect the resource itself, just its appearance in WorkPlace.
11. Click **Next** to move to the **Device Preview** page. This page allows you to see how your layout will appear on different types of devices with different display capabilities. On a mobile device, for example, the **Intranet Address** field cannot be displayed, even if it is configured to be part of a layout.

Network Tunnel Client Configuration

This section describes how to configure settings for the Connect Tunnel client and the OnDemand Tunnel agent.

- IP Address Allocation
- Session Persistence
- Redirection Modes
- Proxy Server Redirection
- ESP Mode
- Secure Network Detection
- Windows Tunnel Client Automatic Client Updating
- Session Termination
- Configuring Tunnel Client Settings

IP Address Allocation

Configuring the network tunnel service to manage TCP/IP connections from the network tunnel clients requires setting up IP address pools for the allocation of IP addresses to the clients. Setting up the address pools is typically done when you configure the network tunnel service. For information on how to initially set up IP address pools, see Configuring IP Address Pools.

When you create communities that will deploy the network tunnel clients to users, you must specify which of those IP address pools are available to members of that community. By default, AMC makes all configured address pools available; however, you can select specific IP address pools if necessary.

Session Persistence

The tunnel clients automatically handle the sorts of connection interruptions that users (and especially mobile users) are familiar with, like undocking a laptop and taking it into a meeting or crossing cellular network boundaries while on the road. Users can experience these temporary interruptions and then resume their sessions without having to reauthenticate.

To allow sessions to be reestablished automatically when a user’s IP address changes (for example, when moving from the office to home), select the **Allow user to resume session from multiple IP addresses** checkbox when you set up EPC zones. See the steps described in Creating a Device Zone or Configuring the Default Zone for more information.

Reauthentication is, however, required if this setting is disabled or if any of the following is true:

- The user’s session on the appliance has expired
- The credentials provided (such as a SmartCard) do not persist during suspend/resume

Redirection Modes

When configuring the network tunnel clients, you must specify a redirection mode, which determines how client traffic is redirected to the appliance. The network tunnel service supports these redirection modes:

- Split Tunnel
- Redirect All

Split Tunnel

In **Split Tunnel (less secure)**, traffic bound for resources defined in AMC is redirected through the tunnel, and all other traffic is routed as normal. This is less secure than redirect all mode, but also more convenient for users because it doesn’t interfere with Internet access.

To safeguard against unauthorized access to users’ computers through their Internet connections, which could potentially reach network resources by re-routing through the split tunnel, consider using End Point Control restrictions to require that users’ computers are running personal firewalls or antimalware protection.

When the appliance is configured with split tunnel, you can allow users to decide whether to give preference to local or remote network access. Under **Configure Realm**> **Configure community**> Redirection mode, when you enable **Use tunnel as primary network (Mobile Connect only)** checkbox, all the DNS queries is resolved in AMC.

Redirect All

In **Redirect all (more secure)**, traffic is redirected through the tunnel regardless of how resources are defined in AMC. This option provides enhanced security, blocking users from being able to access any network device during their tunnel sessions. It may also prevent Internet access, depending on your network configuration.

Redirect all mode is more secure than split tunnel redirection. After launching Connect Tunnel in redirect all mode, users can still modify the routing table, but any traffic not in accordance with the redirection list the appliance sent down to the client is immediately dropped. This prevents users from modifying the routing tables on their computers to bypass the appliance and effectively creating their own split tunnel connection back to the network. Once the routing table has been changed by the Connect Tunnel client, modifying the routing table is ineffective. For more information, see Configuring the Network Tunnel Service.

Exclusions

You can override the behavior of **Split Tunnel** or **Redirect All** by specifying exclusions that is used by the community.

Enable **Exclude local network traffic by default** checkbox if you want to allow users to access local printers and file shares. If corporate resources use the same address space as the local network, they will not be accessible.

Enable **Allow users to exclude or include local network traffic** if you want to allow users to choose local/remote network preference and add custom exclusions. Recommended for advanced users only.

Proxy Server Redirection

Optionally, you can configure traffic bound for the Internet to be redirected through an internal proxy server when the VPN connection is active. This can be useful if you want to use an HTTP proxy server to control remote users' access to Internet resources. This option is available only when the redirect all mode is enabled. For information about configuring these settings, see Configuring Tunnel Client Settings.

Tunnel Clients and Proxy Auto-Configuration Files (Linux Platform)

When OnDemand Tunnel or Connect Tunnel is launched on the Linux platform in an environment where a proxy server is used for outbound access to the Internet, the SMA appliance appends redirection settings to the browser's proxy auto-configuration (`.pac`) file. These modifications are made for the duration of the session only; the original browser settings are reinstated when the user logs out. There are some known issues involving this combination of platform and client:

- In the course of a user's session, one or more prompts may appear requesting approval for changes to the browser's `.pac` file. In order to log in to WorkPlace and ensure proper functionality, the user must accept these `.pac` file modifications.
- If the server `.pac` file is updated, the user must either connect using the OnDemand Tunnel or Connect Tunnel client to incorporate the changes or manually revert to the original proxy settings.
- If a user has a Firefox browser window open when Connect Tunnel is started, the modifications that the appliance needs to make to the browser's `.pac` file (for properly redirecting connections) are not applied to any open browser windows.

  The user must either close and then re-open Firefox or manually reload the browser's proxy settings.

ESP Mode

Encapsulating Security Payload (ESP) is a way to encapsulate and decapsulate packets inside of a UDP wrapper (port 4500) for traversing NATs. Using it can improve the performance of UDP-streaming applications like VoIP. For more information on ESP, see RFCs 2406 and 3948:

http://www.ietf.org/rfc/rfc2406.txt

http://www.ietf.org/rfc/rfc3948.txt

ESP encapsulation is the default setting for newly defined communities. UDP port 4500 must be open in network firewalls for traffic to and from the appliance's external IP addresses and virtual IP addresses when using it.

When enabled, ESP use is automatically negotiated between a client and the SMA appliance. You can choose to use it for all traffic or just UDP traffic; if ESP fails or if the client does not support it, then the SSL tunnel is automatically used instead. The **User Sessions** page in AMC indicates which type of tunnel is being used.

The log files also indicate which tunnel was used: log messages will indicate UDP port 4500 packets for ESP traffic and TCP port 443 packets for SSL tunnel packets.

Under **Configure Realm** > **Configure Community**> **Advanced**> **ESP mode**, you can select **Enable ESP encapsulation of tunnel network traffic** checkbox to improve the performance of the application.

- **Use for all network traffic**
- **Use for UDP traffic only**

Secure Network Detection

Secure Network Detection allows users to automatically establish a tunnel connection when attempting to login from an unsecure location. The client determines the secure network either by connecting to an internal secure host or by matching the client's DNS suffices and servers. Depending on this comparison, the following occurs:

Secure Network Detection

	If connected...	**If not connected...**
Secure host reachable/DNS entry found	Disconnect and reconnect in SND state	Connect in SND state
Secure host reachable/DNS entry not found	Leave connected	Connect using dialer

Secure Network Detection (SND) is provided by Connect Tunnel and Mobile Connect. SND allows secure “always on, always connected” SSL VPN sessions to SMA appliances from client endpoint devices. When Secure Network Detection is enabled, the Connect Tunnel client can detect when the user is located on a non-secure network and automatically establish a tunnel connection. Mobile connect still follows DNS suffix entry for detecting secure network.

The connection status is indicated by an icon on the systray:

Systray Icon	**Description**
🟩	Connected
🟧	Disconnected
🟦	Secure Network

Consider the following when using SND:

- At the EPC Zone level, the **Allow user to resume session from multiple IP addresses** checkbox must be checked for SND to work.
- When enabling Secure Network Detection without Credential Caching, the user may be prompted for their credentials when they transition from secure to non-secure networks (or vice-versa) if their session has been alive longer than the maximum **Credential lifetime** length under **General Settings > Appliance Options**.

For more information on how secure network hosts are used to detect SND, refer to the Secure Network Detection section.

Post-Connection Scripting

You can configure the client to launch an executable file or script on Windows, macOS, or Linux computers after a network tunnel connection has been established. For example, you could specify a Windows `.bat` file that executes a command script that maps network drives. You can also specify command-line options to run when the script launches.

The appliance does not provision the script to users: the client simply executes the script with any specified command-line options. The specified script must already be present on users' computers before the client can execute it, and any specified scripts must be deployed and managed separately.

ⓘ **NOTE:** The post connection script file must be in a location on the client computer that the user can access and where that user can execute files.

For information about configuring these settings, see Configuring Tunnel Client Settings.

Windows Tunnel Client Automatic Client Updating

For users who are running the Windows version of the Connect Tunnel or OnDemand Tunnel client, you can ensure that they have the most recent version of the client by enabling automatic software updating.

Each time a user starts a Windows tunnel client and authenticates, the current client software version is checked against the newest version available on the appliance. If a newer version is available, the user is alerted that an update is ready for download. You can configure (on a per-community basis) what options a user has for installing client updates:

- Allow the user to choose when to start the update process. The update can be deferred indefinitely; however, the user will see the update alert whenever the tunnel client is started (once per day) until the update is installed.
- Make updates mandatory by either requiring them (the user must accept updates in order to access VPN resources) or enforcing them (the install process begins immediately and the user cannot cancel it).

When a user accepts a tunnel client software update by clicking **Install** in the software-update box, the client software update is automatically downloaded and installed on the user's computer (in the case of Connect Tunnel) or activated (in the case of OnDemand Tunnel). After the installation is complete, the tunnel client automatically restarts. Users do not need to reboot their computers after installing the update.

ⓘ **NOTE:** Connect Tunnel Legacy clients (12.1 clients) will not auto update.

For information about configuring software updating, see Configuring Tunnel Client Settings.

Session Termination

By default, a tunnel client session length of time is configured under **Configure Realm** > **Configure Community** >**Session Termination** by enabling the **Limit session length to credential lifetime** checkbox. Users can leave sessions idle and return to them later without having to re-authenticate. If this is a security risk in your environment, there are a couple of ways to terminate sessions and require users to re-authenticate:

- **Manually**: To see a list of sessions click **User Sessions** in the main navigation menu in AMC, and then choose one of the available termination options. For more information, see Ending User Sessions.
- **Automatically**: You can configure the tunnel client to prompt users to re-authenticate as soon as their credentials expire. When **Limit session length to credential lifetime** is selected during tunnel client configuration, sessions in a given community end and require re-authentication after the length of time specified by **Client security** (on the **System Configuration> General Settings> Appliance Options** page).

  See Configuring Tunnel Client Settings for more information about configuring this option.
- Enable the Inactivity Timer in the End Point Control zone, or in the default zone if End Point Control is not used.

Configuring Tunnel Client Settings

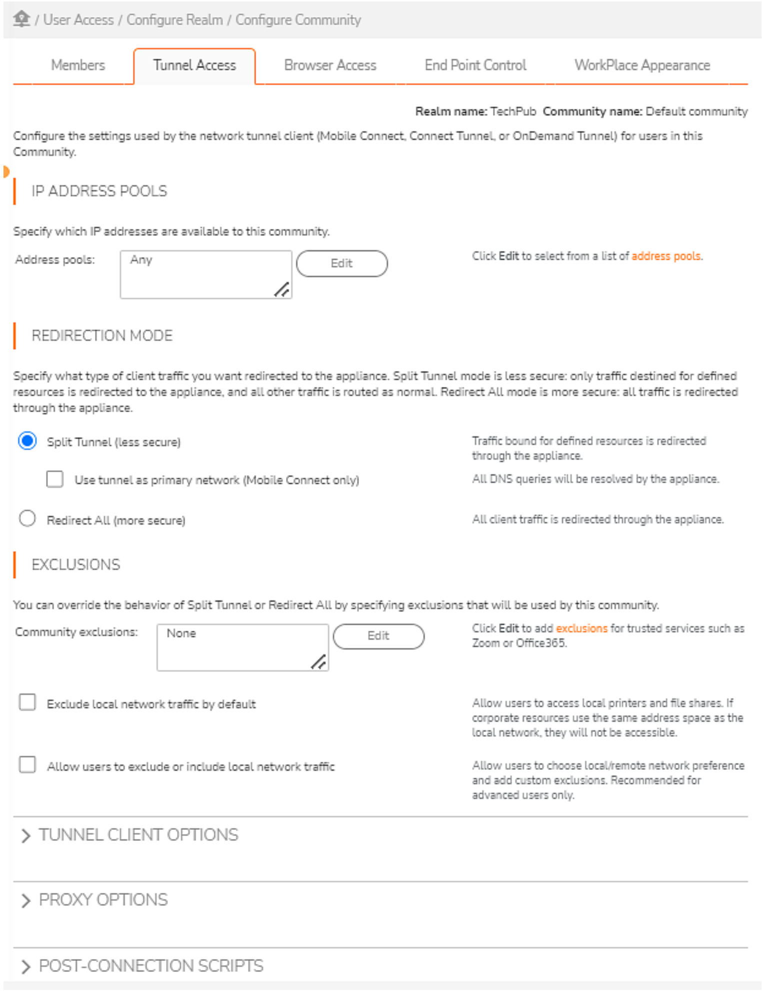
Connect Tunnel is a client application that is installed on a user's device, and OnDemand Tunnel is the same CT client that is activated each time a user logs in to WorkPlace from supported device.

This section describes how to configure settings for the tunnel clients. For a more detailed description of these settings, see Network Tunnel Client Configuration.

To configure tunnel client or agent settings:

1. In the AMC, navigate to **User Access > Realms** and click the link for the community you want to configure, and select **Tunnel Access** tab.

   The **Tunnel Access** page displays.



/ User Access / Configure Realm / Configure Community

Members | Tunnel Access | Browser Access | End Point Control | WorkPlace Appearance

Realm name: TechPub **Community name:** Default community

Configure the settings used by the network tunnel client (Mobile Connect, Connect Tunnel, or OnDemand Tunnel) for users in this Community.

IP ADDRESS POOLS

Specify which IP addresses are available to this community.

Address pools: Any [Edit] Click **Edit** to select from a list of address pools.

REDIRECTION MODE

Specify what type of client traffic you want redirected to the appliance. Split Tunnel mode is less secure: only traffic destined for defined resources is redirected to the appliance, and all other traffic is routed as normal. Redirect All mode is more secure: all traffic is redirected through the appliance.

● Split Tunnel (less secure) — Traffic bound for defined resources is redirected through the appliance.

□ Use tunnel as primary network (Mobile Connect only) — All DNS queries will be resolved by the appliance.

○ Redirect All (more secure) — All client traffic is redirected through the appliance.

EXCLUSIONS

You can override the behavior of Split Tunnel or Redirect All by specifying exclusions that will be used by this community.

Community exclusions: None [Edit] Click **Edit** to add exclusions for trusted services such as Zoom or Office365.

□ Exclude local network traffic by default — Allow users to access local printers and file shares. If corporate resources use the same address space as the local network, they will not be accessible.

□ Allow users to exclude or include local network traffic — Allow users to choose local/remote network preference and add custom exclusions. Recommended for advanced users only.

> TUNNEL CLIENT OPTIONS

> PROXY OPTIONS

> POST-CONNECTION SCRIPTS

2. a. By default, any configured IP address pool is available to the selected community. To select specific IP address pools, click **Edit** in the IP address pools area and then select from the list of configured pools.

   b. Select the Redirection mode used to route client traffic to the appliance. The network tunnel service supports several two redirection modes. For a more detailed description of the supported redirection modes, see Redirection Modes.

      - Split Tunnel (less secure): Traffic bound for resources defined in AMC is redirected through the tunnel, and all other traffic is routed as normal.
        - Enable **Use tunnel as primary network (Mobile Connect only)**checkbox. The appliance will resolve all the DNS queries when you enable the checkbox.
      - Redirect All (more secure): Traffic is redirected through the tunnel regardless of how resources are defined in AMC.

   c. You can override the behavior of Split Tunnel or Redirect All by specifying exclusions that will be used by this community.

In the **Community Exclusions** field, enter the host names, IP addresses, subnets, and IP ranges that you want to exclude from being redirected through the appliance. Wildcard characters (* and ?) are permitted.

ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

ⓘ **NOTE:** For example, if you have three public web servers (www.YourCompany.com, www2.YourCompany.com, and www3.YourCompany.com), you can allow the network traffic associated with them to avoid the appliance, which will improve performance. Add all three public sites to the Exclusions by using a wildcard character: www?.YourCompany.com. Resources in this list can also contain variables; see Using Variables in Resource an WorkPlace Shortcut Definitions for more information.

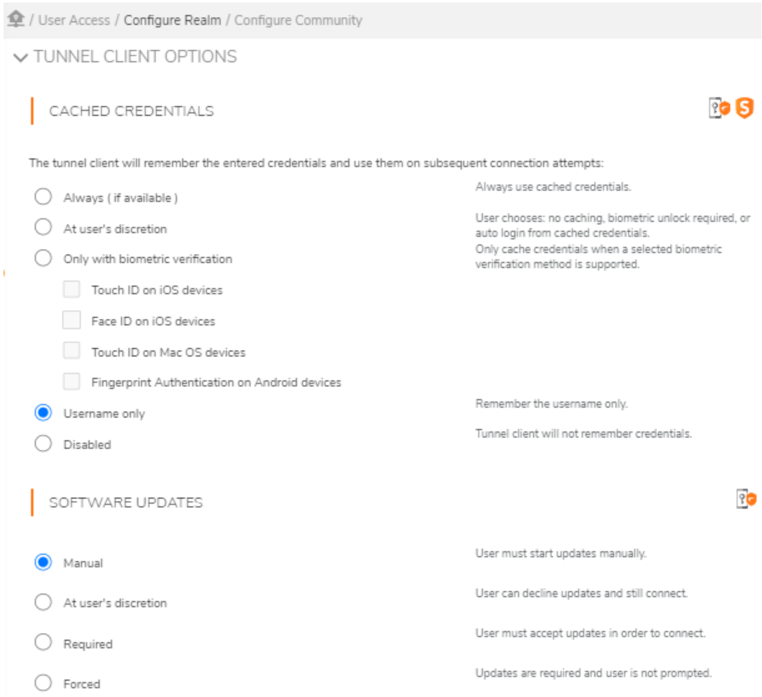
ⓘ **NOTE:** Migration of prior versions of SMA that contains Resource Exclusion List to 12.4.1:

- All entries in Resource Exclusion List migrate to a single exclusion named Split Tunnel
- All Split tunnel communities use this exclusion named Split Tunnel
- For Redirect All communities, exclusions will not be migrated, which may affect browser-only sessions

Enable **Exclude local network traffic by default** checkbox if you want to allow users to access local printers and file shares. If corporate resources use the same address space as the local network, they will not be accessible.

Enable **Allow users to exclude or include local network traffic** if you want to allow users to choose local/remote network preference and add custom exclusions. Recommended for advanced users only.

3. Click to expand the **Tunnel Client Options** section:



/ User Access / Configure Realm / Configure Community

TUNNEL CLIENT OPTIONS

CACHED CREDENTIALS

The tunnel client will remember the entered credentials and use them on subsequent connection attempts:

○ Always (if available)	Always use cached credentials.
○ At user's discretion	User chooses: no caching, biometric unlock required, or auto login from cached credentials.
○ Only with biometric verification	Only cache credentials when a selected biometric verification method is supported.
□ Touch ID on iOS devices	
□ Face ID on iOS devices	
□ Touch ID on Mac OS devices	
□ Fingerprint Authentication on Android devices	
● Username only	Remember the username only.
○ Disabled	Tunnel client will not remember credentials.

SOFTWARE UPDATES

● Manual	User must start updates manually.
○ At user's discretion	User can decline updates and still connect.
○ Required	User must accept updates in order to connect.
○ Forced	Updates are required and user is not prompted.

4. Scroll down to the **Cached Credentials** section and select one of these options:

Option	Description
Always (if available)	Always use cached credentials
At user's discretion	Choose no caching, biometric unlock required, or auto login from cache.
Only with biometric verification	Only use credential caching when biometric verification is supported and enabled. Cached credentials are only used after biometric identification verification.
Username only	Use cached username.
Disabled	Disable cached credentials in the Connect Tunnel client.

ⓘ **NOTE:** On a Windows system, Connect Tunnel uses cached system credentials. On other systems, Connect Tunnel remembers the entered credentials and uses them on subsequent connection attempts.

5. Use one of the **Software updates** options to alert users when client updates are available or update their software automatically. This setting is available only when the network tunnel client is configured to provision client from Secure Mobile Access WorkPlace:

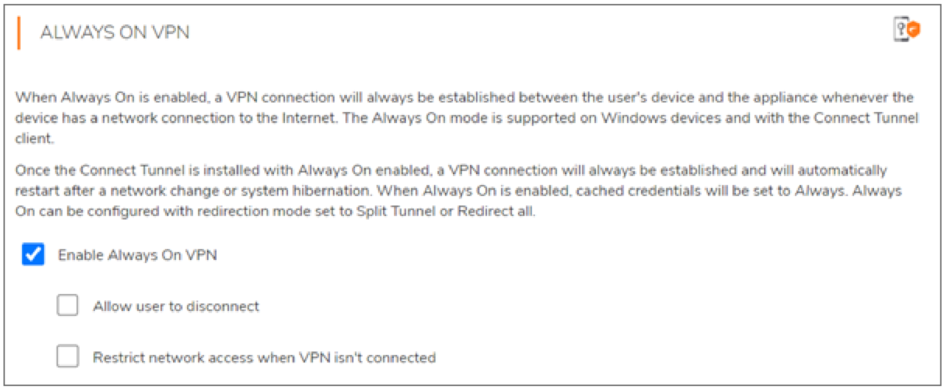
Option	Description
Manual	User must start updates manually.
At user's discretion	Allows users to decide when to install software updates. The update can be deferred indefinitely; however, the user will see the software-update alert when he or she starts the tunnel client (once per day) until the update is installed.

Option	Description
Required	User must accept updates in order to access VPN resources through the tunnel client.
Forced	Updates are required in order to connect. The update program starts, and a progress bar is visible during installation, but the user is not prompted during the process.

6. To automatically establish a tunnel connection when a user attempts to login from an unsecure location, check the **Enable secure network detection** check box in the **Secure Network Detection** section. For more information, see Secure Network Detection.
7. By default, the client is configured to access the realm and appliance name from which the client was downloaded. However, you can override this default behavior and configure the client to access a different realm or appliance. In the **Custom connection** area, select the **Configure client with custom realm and appliance FQDN** check box, and then specify these options as needed:
   - From the **Realm name** list, click the name of the default realm.
   - In the **Appliance FQDN** field, type the fully qualified domain name of the default appliance.
8. By default, a tunnel client session is time specified by **Credential lifetime**by the appliance once it has been established. The default time, is set the **Session Termination** > **Limit session length to credential lifetime.** This requires users to re-authenticate once the amount of time specified by **Credential lifetime** (on the **Configure General Appliance Options** page) has passed. When this option is selected, users are notified when a session is nearing the inactivity threshold and users can avert the disconnect by performing any mouse or keyboard activity.

   If you need a TCP connection or consistent UDP traffic flow between the same two address/port tuples to live longer than eight hours, you must put the user in a community that has this option unchecked. Even with the **Limit session length to credential lifetime** checkbox unchecked, users cannot authorize new flows within the tunnel after their credentials expire.
9. Scroll down to **Always on VPN** section and check the **Enable Always On VPN** box.

   Selecting **Enable Always On VPN** option establishes a VPN connection between the user's device and the appliance whenever the device has a network connection to the internet. You can select the following check boxes, see Device VPN endpoint enrollment



ALWAYS ON VPN

When Always On is enabled, a VPN connection will always be established between the user's device and the appliance whenever the device has a network connection to the Internet. The Always On mode is supported on Windows devices and with the Connect Tunnel client.

Once the Connect Tunnel is installed with Always On enabled, a VPN connection will always be established and will automatically restart after a network change or system hibernation. When Always On is enabled, cached credentials will be set to Always. Always On can be configured with redirection mode set to Split Tunnel or Redirect all.

☑ Enable Always On VPN

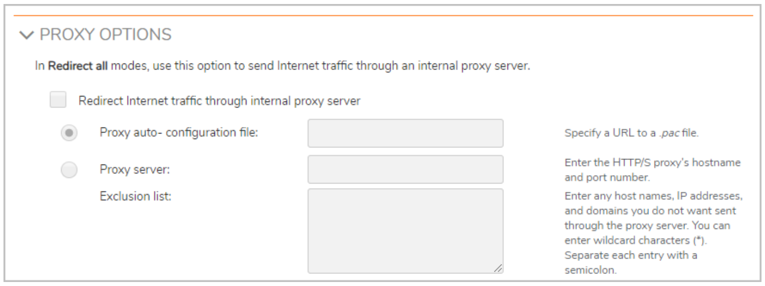
□ Allow user to disconnect

□ Restrict network access when VPN isn't connected

Option	Description
Allow user to disconnect	To allow users to unlock the Connect Tunnel client, disconnect the VPN connection, and modify the Always-on profile.
Restrict network access when VPN is not Connected	To restrict network access to the users until VPN is completely connected.

ⓘ | **NOTE:** Always On VPN is only supported for Connect Tunnel for Windows in SMA 12.4.

10. If you enabled **Redirect all** in the **Redirection mode** area, you can configure Internet traffic to be sent through an internal proxy server when the VPN connection is active. In the **Proxy options** area, select the **Redirect Internet traffic through internal proxy server** checkbox, and then select one of the proxy server options.



PROXY OPTIONS

In **Redirect all** modes, use this option to send Internet traffic through an internal proxy server.

□ Redirect Internet traffic through internal proxy server

● Proxy auto- configuration file: Specify a URL to a *.pac* file.

○ Proxy server: Enter the HTTP/S proxy's hostname and port number.

Exclusion list: Enter any host names, IP addresses, and domains you do not want sent through the proxy server. You can enter wildcard characters (*). Separate each entry with a semicolon.

To specify a proxy auto-configuration (`.pac`) file, click **Proxy auto-configuration file** and then type the URL, preceded by the `http://` protocol identifier, for the `.pac` file. The `.pac` file configures the user's Web browser to load its proxy configuration settings from a JavaScript file rather than from information that you manually specify; the JavaScript file specifies which proxy servers can be used and can redirect specific URLs to specific proxy servers. For information about formatting `.pac` files, see:

http://en.wikipedia.org/wiki/Proxy_auto-confighttp://en.wikipedia.org/wiki/Proxy_auto-config

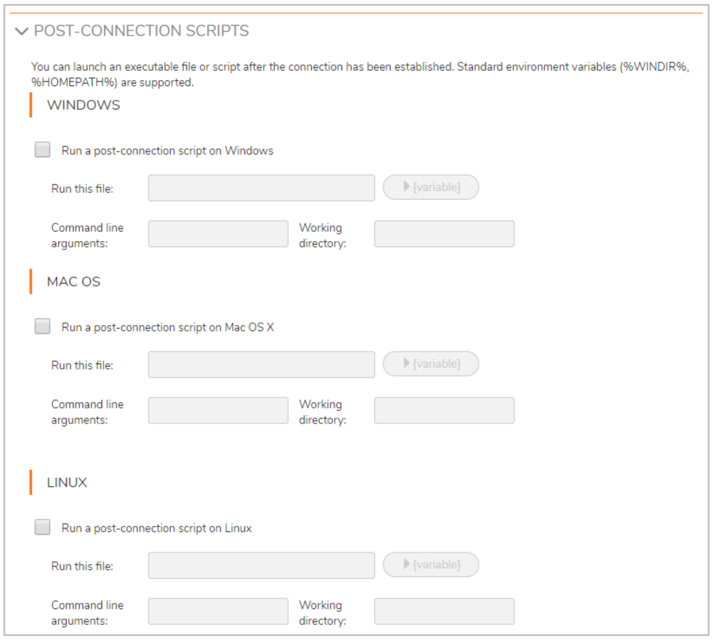
To manually specify a proxy server, click **Proxy server** and then type the server's host name and port number in `host:port` format (for example, `myhost:80`). Optionally, in the **Exclusion list** field, you can type the host names, IP addresses, or domain names of any resources that you do not want redirected through the proxy server. When defining these resources, wild cards are valid, and multiple entries must be separated by semicolons.

11. To launch an executable file or script after the connection has been established:

    a. Click to expand the **Post-connection scripts** area.

    b. Select the **Run a post-connection script** checkbox that corresponds to your operating system.

    c. Specify your settings. For more information, see Post-Connection Scripting.



POST-CONNECTION SCRIPTS

You can launch an executable file or script after the connection has been established. Standard environment variables (%WINDIR%, %HOMEPATH%) are supported.

WINDOWS

□ Run a post-connection script on Windows

Run this file: ▸ {variable}

Command line arguments: Working directory:

MAC OS

□ Run a post-connection script on Mac OS X

Run this file: ▸ {variable}

Command line arguments: Working directory:

LINUX

□ Run a post-connection script on Linux

Run this file: ▸ {variable}

Command line arguments: Working directory:

1. In the **Run this file** field, type the path and name for the script file. For example:

   `%Program Files%\ACME\remote_access.bat`

2. In the **Command line arguments** field, type any command-line arguments that you want to execute when running the script. For example:

   `-user=%USERNAME% -system=%OS%`

3. In the **Working directory** field, type the directory in which the script will be executed. When defining the working directory, you can specify environment variables formatted as `%VariableName%`, where `VariableName` represents the actual environment variable name. For example:

   `%USERPROFILE%\ACME`

ⓘ **NOTE:** The post connection script file must be in a location on the client computer that the user can access and where that user can execute files.

12. In the **Advanced** area, **Enable ESP encapsulation of tunnel network traffic** is selected by default for all network traffic (for all tunnel traffic). ESP (Encapsulating Security Payload) is a way to encapsulate and decapsulate packets inside of UDP packets for traversing Network Address Translators (NATs). Using it can improve the performance of applications, especially UDP-streaming applications like VoIP.

    For an ESP tunnel to function, UDP port 4500 needs to be open in the firewall for traffic to and from the SMA appliance external IP and Virtual IP addresses.

    When ESP is enabled, the tunnel client tries to bring up an ESP tunnel, but falls back to a legacy SSL tunnel if there is a problem establishing the ESP tunnel. The typical reason for this failure is that UDP port 4500 is not open in the network firewall.

    If you do not want to use ESP because you do not want to open UDP port 4500 in your firewall or for any reason, then clear the **Enable ESP encapsulation of tunnel network traffic** checkbox. To disable the default use of ESP in a community, clear the checkbox on the **Realms > [*your tunnel realm*] > Communities > [*your tunnel community*] > Access Methods > Tunnel Access > Advanced**.

13. Click **OK**.

ⓘ | **NOTE:**

- If users are running OnDemand Tunnel in “redirect all” mode, connections to translated Web resources fail with `Page cannot be displayed` errors. To work around this issue, add an A (Address) record to the internal DNS servers to assign the appliance VIP or external IP to the appliance FQDN.
- When **At user’s discretion** is enabled for **Client software updates** in the **Software updates** area, the user sees an upgrade notification, and the Connect Tunnel client caches the user’s response for 24 hours. If the setting is then changed to **Required** or **Forced**, a user who opted to delay updating may not be prompted again until the following day because the earlier response is still cached.
- If you plan to run a VB script after a connection has been established, you cannot simply enter the path and name of the `.vbs` script file; you must use the Windows Script Host utility to invoke it. To work around this, configure the post-connection options as follows:
  - **Run this file**: `<drive>:\windows\system32\cscript.exe`
  - **Command line arguments**: `<Path to script>`. For example:

    `c:\path\to\script.vbs or \\path\to\script.vbs`

  Leave **Working directory** empty.
- When you specify a `.pac` file location, be certain that your tunnel users have access to it. You can do this by defining a resource and creating an access rule. See Creating and Managing Resource Groups and Configuring Access Control Rules.

Connect Tunnel and Captive Portals

Connect Tunnel has the capability to detect a captive portal and, on authentication, Connect Tunnel automatically connects. Many network service providers use captive portals at airports, hotels, or other public places were the Internet services are either paid for, or free only for a limited period of time. Captive portals may require authentication, payment, or the acceptance of a EULA in order for a user to gain general Internet access.

Connect Tunnel looks for an HTTP 302 response status code in order to detect the presence of a captive portal and handle the redirection.

Using the Default Community

After you create a realm, you can create communities with the realm. Communities only exist in the context of one realm, except for the default community, which is shared across all realms. Communities are the mechanism that the appliance uses to deploy access agents and End Point Control components to users.

The easiest way to associate a community with an authentication realm is to use the global Default community that is preconfigured in AMC. The properties automatically assigned to the Default community are:

- Membership in the community is set to **Any**, meaning all users in the authentication realm are assigned to the community.
- Each member of the community is allowed a maximum of 5 active sessions.

- Web-based proxy access (TCP protocol) and Web access (HTTP) methods are made available to community members.
- No End Point Control restrictions are imposed on users' computers.

Changing the Order of Communities Listed in a Realm

When users log in to an authentication realm, the appliance looks up the community to which they belong so that access agents and EPC policy can be deployed to them. If you use only one community per realm or if you ensure that each user is assigned to only one community, then the process of logging in and receiving the appropriate access agent is straightforward.

However, if some users belong to more than one community, the order in which the communities are listed on the **Communities** tab of the **Configure Realm** page determines the community to which those users are assigned , however only one the default community that is available is shared with all realm. The appliance attempts to match users to communities starting at the top of the list. Users are assigned to the first community in the list that they match. The best practice is to place the most specific community at the top of the list.

To change the order of the communities for a realm:

1. From the main navigation menu, click **Realms**.
2. Click the name of the authentication realm whose communities you want to re-order.
   The **General** tab of the **Configure Realm** page displays.
3. Click the **Communities** tab.
   The communities that are part of this realm will be matched in the order that is listed here.
4. Use the **Move Up** or **Move Down** links to move the selected community up or down.
5. When the communities are listed in the order you want, click **Save**.

ⓘ **NOTE:** The community a user is assigned to is displayed on the Secure Mobile Access WorkPlace home page (click **Details** in the **Connection Status** area).

Configuring RADIUS Accounting in a Realm

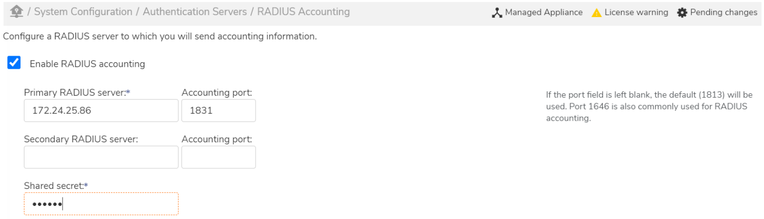
If you use a RADIUS server for collecting accounting information, you can configure a RADIUS accounting server in AMC and then enable accounting on a per-realm basis. The appliance sends RADIUS accounting messages to the server identifying user sessions, the time and duration of their connections, and their source IP addresses.

The appliance can connect to one RADIUS server at a time. If two RADIUS servers are configured in AMC, the appliance sends messages to just the primary server, and communicates with the secondary server only if there is a communication failure with the primary one.

To configure a RADIUS accounting server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In **RADIUS Accounting** click the **Edit** link.

3. To enable the appliance to save RADIUS, syslog, and routing changes, select the **Enable accounting records** checkbox.



/ System Configuration / Authentication Servers / RADIUS Accounting
Managed Appliance
License warning
Pending changes

Configure a RADIUS server to which you will send accounting information.

☑ Enable RADIUS accounting

Primary RADIUS server:* 172.24.25.86

Accounting port: 1831

Secondary RADIUS server:

Accounting port:

Shared secret:* ••••••

If the port field is left blank, the default (1813) will be used. Port 1646 is also commonly used for RADIUS accounting.

4. In the **Primary RADIUS server** field, type the IP address for the primary accounting server. In the **Accounting port** box, type the port number used to communicate with the server. If left blank, AMC uses the default server port (**1813**).
5. If you are using a second RADIUS accounting server as a backup in case communication between the appliance and the server fails, enter the server's IP address in the **Secondary RADIUS server** field, and the port number in the **Accounting port** field.
6. In the **Shared secret** field, enter the shared secret that allows the appliance to communicate with the RADIUS accounting server.
7. In the **Retry interval** field (in the **Advanced** area), type the number of seconds to wait for a reply from the RADIUS server before retrying communication with the server.
8. By default, the appliance uses its appliance name (from the **Configure Network Interfaces** page) to identify itself to the RADIUS accounting server. However, you can use the **NAS-Identifier** and **NAS-IP-Address** boxes to have the appliance send different identity information.
9. In the **Locale encoding** area, do one of the following:
    - Choose a character set from the **Selected** drop-down menu. See Selected RADIUS Character Sets for a list of selected character sets.
    - Click **Other** and then type the name of a character set in the field. See Other Supported RADIUS Character Sets for a list of character sets that can be entered.
10. Click **Save**.

Editing, Copying and Deleting Communities

For information on how to edit, copy, and delete communities, see Adding, Editing, Copying, and Deleting Objects in AMC.

Managing Users and Groups

User and group management is an ongoing job. Although most user management is done through external user repositories (users and groups are not stored directly on the appliance, but are instead referenced), keeping the AMC list current is essential for delivering reliable access.

The users and groups defined in AMC are associated with any directories currently configured on the appliance.

Topics:

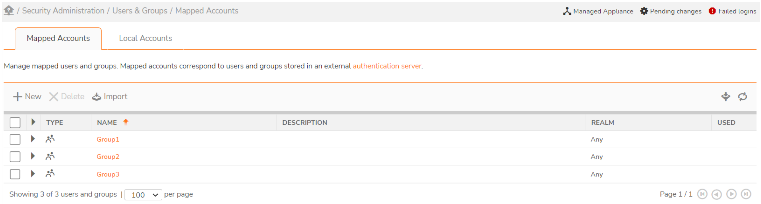
- Viewing Users and Groups
- Managing Users and Groups Mapped to External Repositories
- Managing Local User Accounts

Viewing Users and Groups

Users and groups configured in AMC are displayed on the **Mapped Accounts** and **Local Accounts** pages.

To view users and groups:

1. In the AMC, navigate to **Security Administration > Users & Groups**.



Manage mapped users and groups. Mapped accounts correspond to users and groups stored in an external authentication server.

□		TYPE	NAME	DESCRIPTION	REALM	USED
□	▶	👥	Group1		Any	
□	▶	👥	Group2		Any	
□	▶	👥	Group3		Any	

Showing 3 of 3 users and groups | 100 per page   Page 1 / 1

2. Select the tab for the user object you want to view:

This tab	Lets you
Mapped Accounts	Manage groups of users and individual users mapped to group information stored on an external authentication server. Create new groups based on directory information.
Local Accounts	Manage users stored in a local user-authentication repository on the appliance.

3. Optionally, use the **Filters** settings to display only the objects you are interested in.

   For information about using filters, see Filters.

4. Review the data shown in the list of managed or local accounts:

   - The checkbox column is used to select one or more list items to delete.
   - The plus sign (+) column expands the display of user, group, or local account information.
   - The **Type** column displays an icon identifying whether the object is a 👤 (user) or 👥 (group).
   - The **Name** column displays the name you assigned when creating a user, group, or local user account.
   - The **Description** column shows the text you entered when creating an account.
   - The **Realm** column displays the realm with which a user, group, or local user account is associated.

    - The **Used** column shows whether the user or group is currently in use.

5. Click a column heading to sort the list by that column.

Managing Users and Groups Mapped to External Repositories

Unless defined as members of the local user authentication store, users and groups are not stored directly on the appliance, but are instead referenced from external user directories. In most cases, you manage individual users in AMC only when you need to assign them permissions that are different from those that their group membership allows. There are two ways to form groups of users in AMC using information stored in external directories:

- Use the same group names as the external directory. In most directories, similar user accounts are grouped together so they can be granted similar rights and permissions. Assuming that your directory is organized in this way, your user management on the appliance is usually centered around groups, not users. Set up the appliance to reference user groups stored in your directory, and then reference those groups in access control rules.
- Query the external directory using common attributes. The results can be used to create a new group (one that is not referenced in the external directory) that can be used in access control rules. You might create a new group named “Local employees” by querying the directory for all employees living within a given set of zip codes.

For Microsoft Active Directory and LDAP directories, there are several ways to add groups (this feature is not available for adding users referenced by a RADIUS realm or in the local user store):

- Manually type a distinguished name (DN)
- Search the contents of the directory and select groups from a list
- Build a dynamic group expression

For testing and evaluation purposes, you can also create local users on the appliance. See Managing Local User Accounts.

Topics:

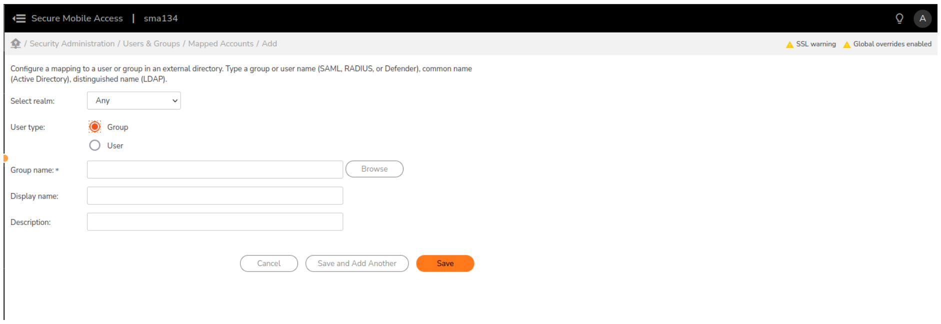
- Adding Users or Groups Manually
- Importing users and groups csv file in mapped accounts
- Adding Users or Groups by Searching a Directory
- Advanced Search Methods
- Creating Dynamic Groups Using a Directory
- Editing Users or Groups
- Deleting Users or Groups

Adding Users or Groups Manually

When you create an access control rule, one of the things you do is specify the users and groups to which a given rule applies. You must add users before you can specify them in access control rules. Users can be added manually or by using the Active Directory or LDAP directory. To use a directory, click **Browse** to search the directory. See Adding Users or Groups by Searching a Directory for more information.

To add a user manually:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Select the **Mapped Accounts** tab
3. Click the **+**(New) icon.
4. Select **Manual entry** from the dropdown menu.


Secure Mobile Access | sma134
/ Security Administration / Users & Groups / Mapped Accounts / Add
SSL warning
Global overrides enabled
Browse
Cancel
Save and Add Another
Save

Configure a mapping to a user or group in an external directory. Type a group or user name (SAML, RADIUS, or Defender), common name (Active Directory), distinguished name (LDAP).

Select realm: Any

User type: ● Group ○ User

Group name: *

Display name:

Description:

5. In the **Select realm** drop-down menu, select the realm to which the user belongs. If the user exists in multiple realms and you want the appliance to search for any occurrence, select **Any** from the realm list.
6. In the **User type**, select the type of account to add: **Group** (default) or **User**.
7. If you selected **Group**, in the **Group name** field type the group name exactly as it appears in the external repository. (Group names are case-sensitive). The name depends on the type of directory to which you are mapping:

Directory type	**What to type**
LDAP	Type a distinguished name (DN). For example: `cn=Sales,cn=Users,dc=example,dc=com`
Active Directory	Type a common name (CN) or distinguished name (DN). A CN is easier to enter than a DN (for example, you can type `Sales` instead of: `cn=Sales,cn=Users,dc=example,dc=com`) but the CN is not guaranteed to be a unique match. When in doubt, it's best to use a DN.
RADIUS	Type a group name. For example, `Sales`.

When you specify an Active Directory or LDAP group, its sub-groups (if any) are also included. The number of nesting levels that you want to include when evaluating group membership is configured when you set up an authentication server; see Configuring LDAP with Username and Password and Configuring Active Directory with Username and Password for more information.

NOTE: When using an external directory for authentication and you add a user group in AMC, you are not actually grouping users. You are merely adding the name of a user group that is defined in your external user repository.

The appliance also supports local users and groups. See Managing Local User Accounts.

8. If you selected **User**, for the **User name**, type the user name exactly as it appears in the external repository. User names are case-sensitive; the following table explains the syntax used to define users.

Name Selection

Directory type	What to enter
Active Directory or RADIUS	Type a user name. For example, `jsmith`.
LDAP	Type a distinguished name (DN). For example: `cn=jsmith,cn=Users,dc=example,dc=com`

9. (Optional) In the **Display name** field, type the name to display in AMC pages to identify the group or user.
10. (Optional) In the **Description** field, type a descriptive comment about the group or user.
11. Click **Save** or **Save and Add Another**.

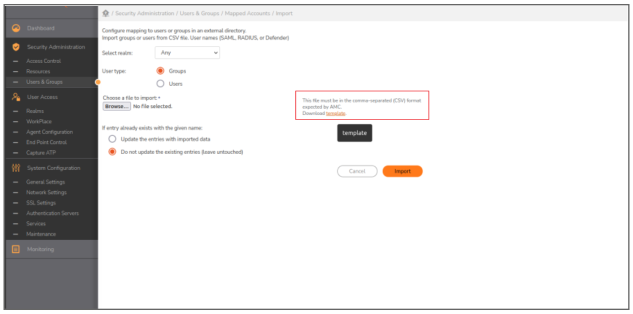
NOTE: If you enter the name incorrectly the user will not be authorized to access any resources.

Importing users and groups csv file in mapped accounts

To import the users and groups csv file:

1. In the AMC, navigate to **Security Administration** > **Users & Groups**.
2. Click the **Mapped Accounts** tab.
3. Click the **Import** button.

   The **Import** page is displayed.
4. Click **Download Template**.



/ Security Administration / Users & Groups / Mapped Accounts / Import

Configure mapping to users or groups in an external directory.
Import groups or users from CSV file. User names (SAML, RADIUS, or Defender)

Select realm: Any

User type: ● Groups ○ Users

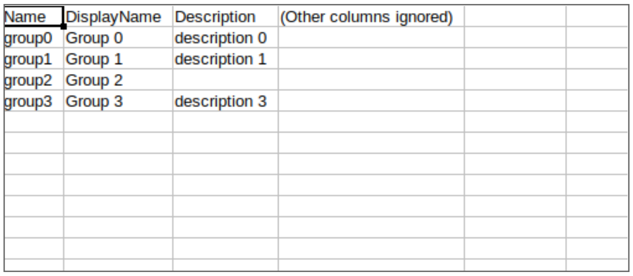
Choose a file to import: *
Browse... No file selected.

This file must be in the comma-separated (CSV) format expected by AMC.
Download template.

If entry already exists with the given name:
○ Update the entries with imported data
● Do not update the existing entries (leave untouched)

5. Open the downloaded .csv file and add users or groups from second row.

NOTE: You can either import users or groups .csv file.
The first row in .csv file is for heading and is not considered during import.

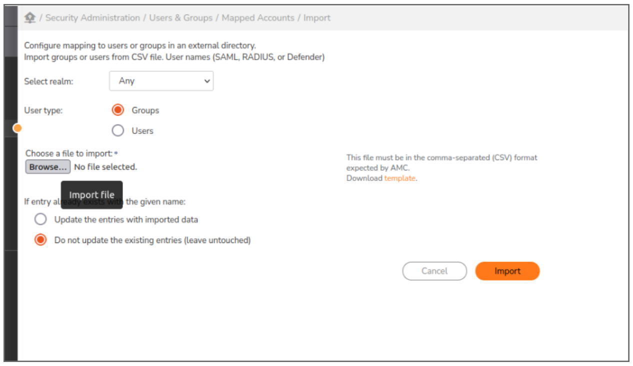


Name	DisplayName	Description	(Other columns ignored)
group0	Group 0	description 0	
group1	Group 1	description 1	
group2	Group 2		
group3	Group 3	description 3	

6. Fill in the first column.

   ⓘ | **TIP:** It is optional to fill the second and third columns.

7. Click **Save** and close the .csv file.
8. In the **Import** page, select any realm or **Any** in **Select realm** option.
9. In **User Type** select any one of the **Groups** or **Users** options.
10. Click on the **Browse** button and select the saved .csv file.
11. Under the **If entry already exists with the given name** option, choose any one the following:
    - **Update the entries with imported data**
    - **Do not update the existing entries**
12. Click **Import**.



/ Security Administration / Users & Groups / Mapped Accounts / Import

Configure mapping to users or groups in an external directory.
Import groups or users from CSV file. User names (SAML, RADIUS, or Defender)

Select realm: Any

User type: ● Groups ○ Users

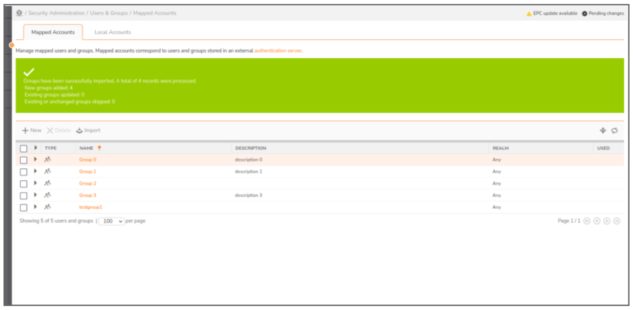
Choose a file to import: *
Browse... No file selected.

This file must be in the comma-separated (CSV) format expected by AMC.
Download template.

If entry al[ready exists with] the given name:

○ Update the entries with imported data
● Do not update the existing entries (leave untouched)

All the users or groups are imported and report is displayed.



Manage mapped users and groups. Mapped accounts correspond to users and groups stored in an external authentication server.

Groups have been successfully imported. A total of 4 records were processed.
New groups added: 4
Existing groups updated: 0
Existing or unchanged groups skipped: 0

TYPE	NAME	DESCRIPTION	REALM	USED
	Group 0	description 0	Any	
	Group 1	description 1	Any	
	Group 2		Any	
	Group 3	description 3	Any	
	testgroup1		Any	

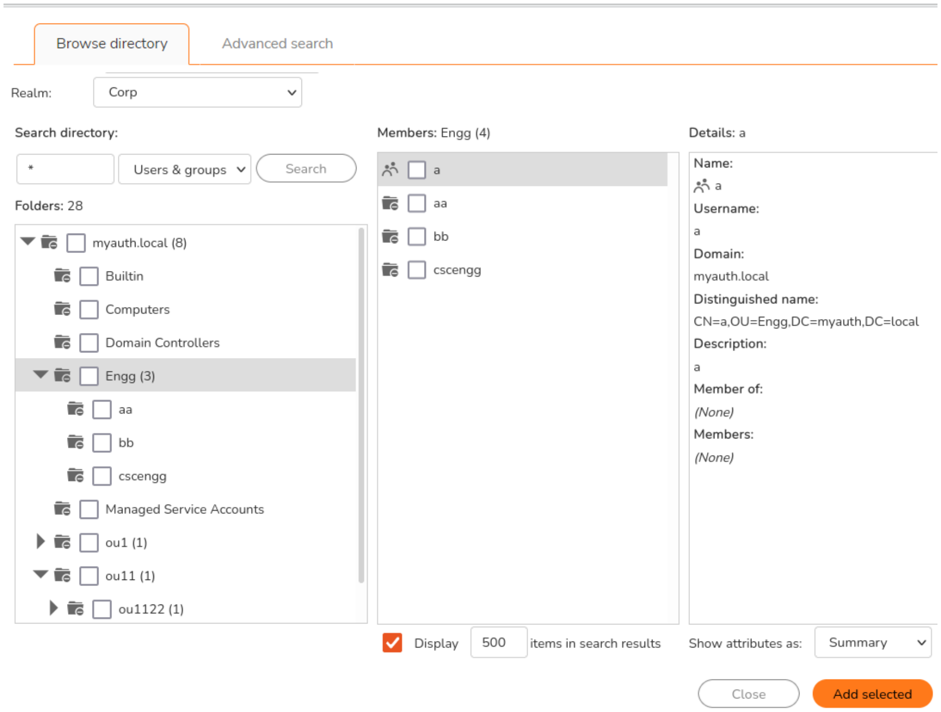
Showing 5 of 5 users and groups | 100 per page — Page 1 / 1

Adding Users or Groups by Searching a Directory

The most common way to add groups in AMC is to browse an external directory and add matching groups.

To add a user or group by searching a directory:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Select the **Mapped Accounts** tab.
3. Click the **+** (New) icon.
4. Select **Directory search** from the dropdown menu.



Realm: Corp

Search directory: * Users & groups

Folders: 28

- □ myauth.local (8)
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ Engg (3)
    - □ aa
    - □ bb
    - □ cscengg
  - □ Managed Service Accounts
  - □ ou1 (1)
  - □ ou11 (1)
    - □ ou1122 (1)

Members: Engg (4)

- □ a
- □ aa
- □ bb
- □ cscengg

Details: a

Name:
a
Username:
a
Domain:
myauth.local
Distinguished name:
CN=a,OU=Engg,DC=myauth,DC=local
Description:
a
Member of:
(None)
Members:
(None)

☑ Display 500 items in search results

Show attributes as: Summary

5. Select the realm you want to search (only realms that use an Active Directory, Active Directory Tree, or LDAP authentication server are available).

   If you select a realm that uses an authentication server on which group checking is disabled, the **Search** field is not clickable and the message `Group checking has been disabled for this realm` is displayed. See Disabling Authorization Checks for more information.

6. If the realm you selected uses an Active Directory Tree authentication server, select the domain you want to search.
7. Define your search criteria:
   - In the **Search directory** field, type all or part of a user or group name. The default is `*`, which returns all records in the repository. You can use the wild card character (`*`) anywhere in the search string. For example, to find group names beginning with the letter `j`, you would type `j*`. Or,

to find users named `Mary` or `Marty` (but not Max), you could type `m*y`.

- To narrow your search, type the name and select **Groups only** or **Users only** from the drop-down menu. For example, you might type `sn` to look for a user's surname or `cn` to find a common name.
- To specify more detailed search criteria, click the **Advanced** tab; see Advanced Search Methods for details.

8. Click **Search**, which displays all matches in the second column.
9. Locate the objects you want to add:
   - Change the filter options to view the records.
   - To view detailed information about a user or group, click its name. A detailed list of attributes appears in the right-hand pane. If a group is nested, click the sub-group to see its details:

     The number of nested levels that it is possible to display is configured when you set up an authentication server; see Configuring LDAP with Username and Password and Configuring Active Directory with Username and Password for more information.
   - Select the checkbox to the left of any users or groups you want to add to the appliance.
10. To add selections to the appliance, click the **Add Selected** button.

    The items are added to the list on the appropriate page (**Groups** or **Users**) in alphabetical order.
11. When you're finished, click the **Close** button in the upper right to close the **Search Directory** page.

ⓘ **NOTE:** By default, the basic search is configured to locate users and groups by querying the **sAMAccountName**, **cn**, **uid**, and **userid** attributes.

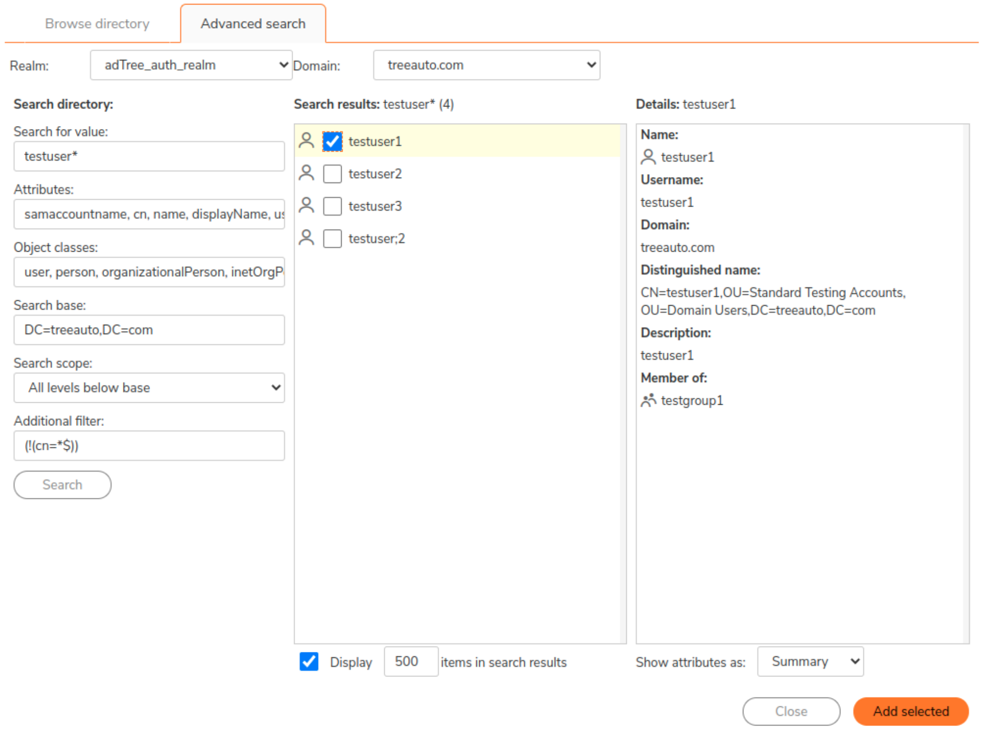
Most chained authentication deployments involve an LDAP or AD server paired with another authentication server (like RADIUS). In the unlikely event that you are using chained authentication with a combination of LDAP and AD servers, keep the following in mind:

- If you are searching for users, only search results from the first LDAP or AD authentication server in the chain are displayed. The policy server, however, returns results from both servers in the chain.
- The same is true when searching for groups (except if an affinity server is configured for the realm: it will be searched instead of the authentication servers).

For example, if you have a group called *Accounting* on both LDAP or AD servers in your chained authentication, any access control rules you create that are restricted to the Accounting group applies to group members on both servers, even though the Search Directory page shows results from just the first server in the chain.

Advanced Search Methods

If you are familiar with LDAP syntax, you can create an advanced search to further narrow the scope of your query. This is especially useful when querying a large directory. In some cases, you may also need to perform an advanced search to query a directory using a non-standard schema. To perform an advanced search, click the **Advanced search** tab.



Realm: adTree_auth_realm
Domain: treeauto.com

Search directory:

Search for value: testuser*

Attributes: samaccountname, cn, name, displayName, us

Object classes: user, person, organizationalPerson, inetOrgP

Search base: DC=treeauto,DC=com

Search scope: All levels below base

Additional filter: (!(cn=*$))

Search results: testuser* (4)

- ☑ testuser1
- □ testuser2
- □ testuser3
- □ testuser;2

Details: testuser1

Name:
testuser1
Username:
testuser1
Domain:
treeauto.com
Distinguished name:
CN=testuser1,OU=Standard Testing Accounts, OU=Domain Users,DC=treeauto,DC=com
Description:
testuser1
Member of:
testgroup1

☑ Display 500 items in search results

Show attributes as: Summary

The fields used to specify advanced search criteria are explained in the Advanced search criteria table:

Advanced Search Criteria

In this field	You
Search for value	Specify an LDAP search filter to reduce the scope of the search. Type all or part of a user or group name. The default is `*`, which returns all records in the realm. You can use the wild card character (*) anywhere in the search string. For example, to find group names beginning with the letter `j`, you would type `j*`. Or, to find users named `Mary` or `Marty` (but not `Max`), you could type `m*y`.
Attributes	Select an LDAP attribute. For example, you might select **sn** to look for a user's surname or **cn** to find a common name.
Object classes	Specify the object class containing users or groups. For users, this is typically `user` or `inetOrgPerson`. For groups, this is usually `group`, `groupOfNames`, or `groupOfUniqueNames`.

<table>
<tr><td>Search base</td><td>Enter the point in the LDAP directory from which to begin searching. Usually, this is the lowest point in the directory tree that contains users or groups.
For LDAP, you might type <code>ou=Users,o=example.com</code>.
To search Microsoft Active Directory, you might use
<code>CN=users,DC=example,DC=corp,DC=com</code>.</td></tr>
<tr><td>Search scope</td><td>Select the containers that you want to search:
<b>All levels below base</b> (default) – retrieves information from all levels below the search base. The search base itself is not included in this scope.
<b>One level below base</b> – Retrieves information from one level below the search base. The search base itself is not included in this scope.</td></tr>
<tr><td>Additional filter</td><td>Specify an LDAP search filter to reduce the scope of the search:</td></tr>
<tr><td></td><td><b>Syntax</b>:
<code>(filter=(operator(LDAP attribute=value)(..)))</code>
<b>Operators</b>:
• OR = <code>|</code>
• AND = <code>&</code>
• NOT = <code>!</code>
<b>Examples</b>:
<code>(cn=Sandy Cane)</code>
<code>(!(cn=Tim Howes))</code>
<code>(&(objectClass=Person)(|(sn=Cane)(cn=Sandy C*)))</code></td></tr>
</table>

ⓘ | **NOTE:** For more information on LDAP search filters, see RFC 2254 at http://www.ietf.org/rfc/rfc2254.txt.

The LDAP search syntax is flexible and provides several ways to accomplish the same result. For example, you might use the object class to search for all groups in a directory:

```
objectclass=group;groupOfNames
```

Alternatively, you can get the same result using a search filter:

```
(|(objectclass=group)(objectclass=groupOfNames))
```

Creating Dynamic Groups Using a Directory

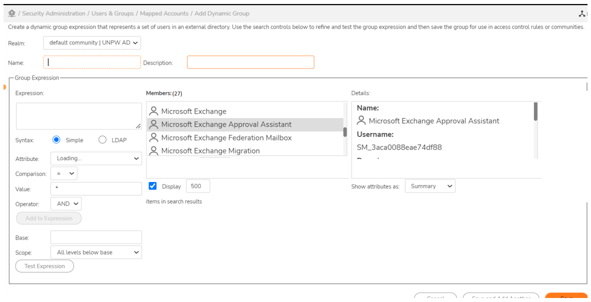
If you are using an external Microsoft Active Directory or LDAP directory, you can form AMC groups by building your own directory query or, if you're familiar with LDAP syntax, writing your own directory query.

Dynamic groups are useful if you want to create a policy that applies to a group that is not already defined in the external directory. For example, you might want to create a group called *Operations* (*Seattle*). Although the external directory might already have a group called *Operations*, you want to narrow it down to members who are based in Seattle.

To add a dynamic group using an external directory:

IMPORTANT: When conducting a multi-valued query against an LDAP or AD directory, you must specify the full DN of the group being queried.

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. On the **Mapped Accounts** tab, click **New** and then select **Dynamic group**.

   / Security Administration / Users & Groups / Mapped Accounts / Add Dynamic Group

   Create a dynamic group expression that represents a set of users in an external directory. Use the search controls below to refine and test the group expression and then save the group for use in access control rules or communities.

   Realm: default community | UNPW AD

   Name:

   Description:

   Group Expression

   Expression:

   Syntax: ● Simple ○ LDAP

   Attribute: Loading...

   Comparison: =

   Value: *

   Operator: AND

   Base:

   Scope: All levels below base

   Members: (27)

   Microsoft Exchange
   Microsoft Exchange Approval Assistant
   Microsoft Exchange Federation Mailbox
   Microsoft Exchange Migration

   ☑ Display 500 items in search results

   Details:

   Name:
   Microsoft Exchange Approval Assistant
   Username:
   SM_3aca0088eae74df88

   Show attributes as: Summary

   Users who match the expression that you build or write in this page are dynamically included in this group. If a user is added later and matches this expression, it is automatically included in this group.
3. Select the realm to which this new group belongs from the **Realm** drop-down menu. Only realms that have been configured with an Active Directory or LDAP server (single or chained authentication) are available.
4. (Optional) Type a **Name** for this dynamic group.
5. Optionally, type a **Description** that can be used when creating access rules that apply to only certain groups.
6. Use these fields in the **Group Expression** area to build your query (see the Advanced Search Methods table for help with LDAP query syntax):

   Fields Usage

Setting	Description
Expression	The query you create using the following fields is displayed here so that you can edit it (if necessary).
Syntax	Choose between **Simple** and **LDAP** syntax.

Attribute	An initial query is sent to the external directory server to get a list of defined attributes. (If this list does not look correct, check the name of the realm you selected in the **Realm** list.)
Comparison	A menu of commonly used LDAP search operators (=, !=, >=, and <=) to filter the values returned by the LDAP or Active Directory server.
Value	A user-entered value that can contain wild cards (*****). Assuming an **Attribute** of *ZipCode*, for example, you could type a **Value** of `98*` to query for all employees living in Washington state.
Operator	Common logical operators (**AND**, **OR**).
Add to Expression	Adds the current attribute, value, and operator to the **Expression** text area. You can cycle back through (as many times as needed), defining an additional **Attribute**, **Value**, and **Operator** to further refine your query. Click **Add to Expression** after each addition.
Base	(Optional) Base of the AD/LDAP authentication server. It specifies the point in the LDAP directory from where to start the query. For example, to search users in the Microsoft Active Directory: `CN=users, DC=engineering, DC=sonicwall, DC=com` If a base is not entered, the query is performed at the search based of the authentication server.
Scope	Depth of the query. Selecting **All levels below base** (default) to retrieve information from all levels below the base. Select **One level below base** to retrieve information from the search base itself. No containers below the search base are searched.

You can also type a query directly in the **Expression** field.

7. Click **Test Expression** to test the expression created.

   The results are displayed in the Members section To limit the number of members displayed, check the **Display** checkbox and typing the maximum number of items in the **Display** field.

   Testing an expression sends the LDAP search query displayed in the **Expression** area to the LDAP or AD server and displays the results (a list of users) in the right-hand pane. If the results are not what you expect, modify the query by either building the expression or editing the query directly in the **Expression** field and then test again.

   ⓘ | **TIP:** A new group should not be saved until the expression has been tested.

8. Use the **Show attributes as** drop-down menu in the lower right corner of the page to display details in the **Details** section about the member selected in the **Members** section. Selecting **Summary** shows a summary of the member, and selecting **All attributes** shows all attributes of the member.

   ⓘ | **NOTE:** Most chained authentication deployments involve an LDAP or AD server paired with another authentication server (like RADIUS). In the unlikely event that you are using chained authentication with a combination of LDAP and AD servers, keep the following in mind:

   - If you are searching for users, only search results from the first LDAP or AD authentication server in the chain are displayed. The policy server, however, will return results from both servers in the chain.

- The same is true when searching for groups (except if an affinity server is configured for the realm: it will be searched instead of the authentication servers).

For example, if you have a group called *Accounting* on both LDAP or AD servers in your chained authentication, any access control rules you create that are restricted to the *Accounting* group will apply to group members on both servers, even though the **Search Directory** page shows results from just the first server in the chain.

Editing Users or Groups

If a user or group name or distinguished name changes in your external directory, you must modify the account on the appliance. You can also change local user accounts or group names on the appliance. For information about editing local accounts, see Managing Local User Accounts.

To edit a user or group:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Mapped Accounts** tab, and then click the name of the group or user that you want to edit.

   The **Edit Mapped Account** page displays.
3. Make any edits as needed. If the user or group is in an Active Directory or LDAP realm, you can click **Browse** and then search for the user.
4. Click **Save**.

Deleting Users or Groups

ⓘ **NOTE:** You cannot delete a user or group if it is referenced by another object. See Deleting Referenced Objects for more details.

When you delete a user or group that is mapped to an external user directory, its mapping is removed from the system. Deleting a user or group mapping does not remove the user or group from the external user directory. For information about deleting local users or group, see Managing Local User Accounts.

To delete a user or group:

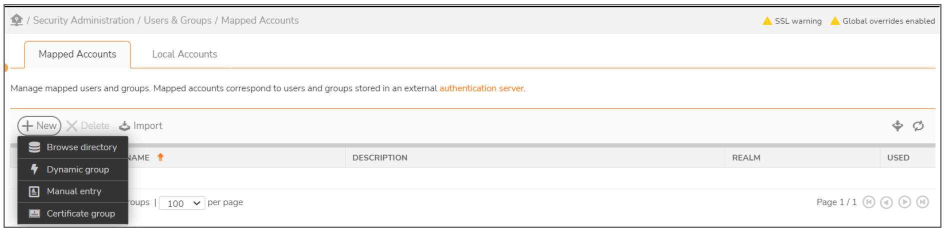
1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Mapped Accounts** tab.
3. Select the checkbox to the left of any groups or users that you want to delete.
4. Click the **X** (Delete) icon.

Certificate Group

Introduced an administrator interface to create a certificate group and assign users to the group. You can assign multiples users from different communities for realms and enable them with a common privilege to use the PKI authentication server.

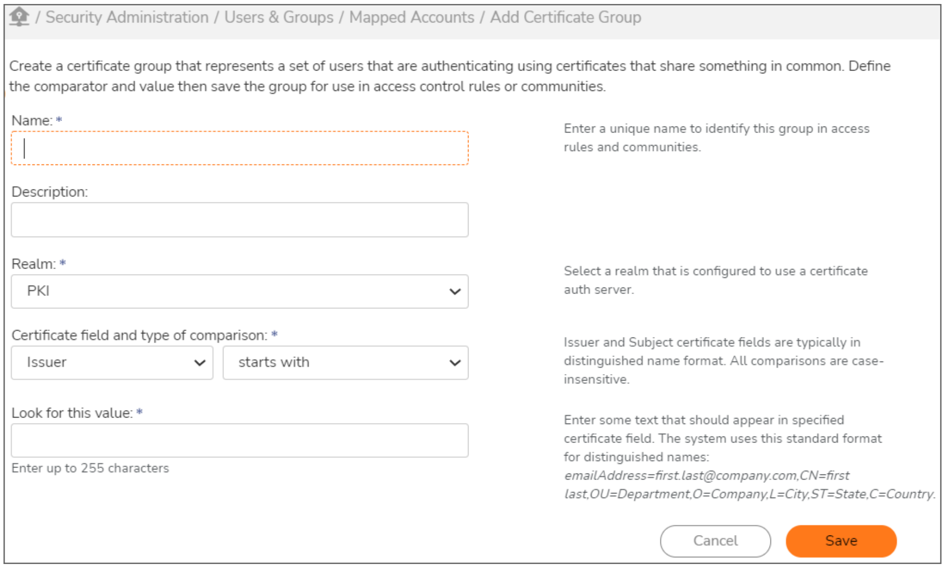
To create a certificate group:

1. Log in to AMC.
2. Navigate to **Security Administration > Users & Groups**.
3. In the **Mapped Accounts** tab, click + icon and select **Certificate Group** option.



Manage mapped users and groups. Mapped accounts correspond to users and groups stored in an external authentication server.

4. In the **Name** field, enter a unique name to identify this group in access rules and communities.
5. In the **Description**, enter the description for the certificate group.
6. In the **Realm**, select **Device VPN**.
7. Select the certificate field and type of comparison from the respective drop-down box.
8. In the **Look for this value** field, enter the text that should be present in the certificate.
   The system uses this standard format for distinguished names:
   emailAddress=first.last@company.com,CN=first last,OU=Department,O=Company,L=City,ST=State,C=Country.
9. Click **Save**.
   Once the certificate group is created, you can select the certificate group when creating access control rules or when selecting the members of a community.


/ Security Administration / Users & Groups / Mapped Accounts / Add Certificate Group
Cancel
Save

Create a certificate group that represents a set of users that are authenticating using certificates that share something in common. Define the comparator and value then save the group for use in access control rules or communities.

Name: *

Enter a unique name to identify this group in access rules and communities.

Description:

Realm: * PKI

Select a realm that is configured to use a certificate auth server.

Certificate field and type of comparison: * Issuer starts with

Issuer and Subject certificate fields are typically in distinguished name format. All comparisons are case-insensitive.

Look for this value: *

Enter up to 255 characters

Enter some text that should appear in specified certificate field. The system uses this standard format for distinguished names: *emailAddress=first.last@company.com,CN=first last,OU=Department,O=Company,L=City,ST=State,C=Country.*

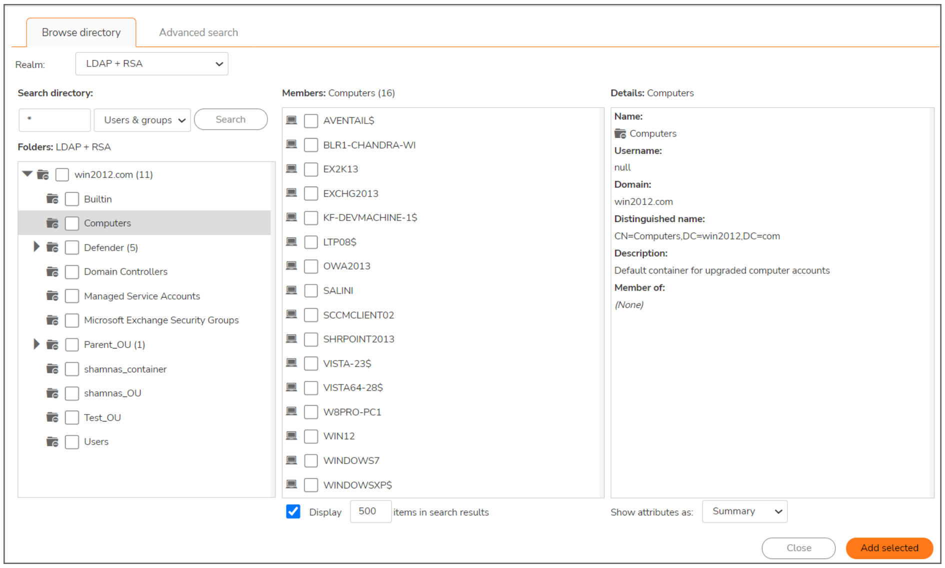
Support for Domain Computers in AD server as VPN users

You can now select the domain computers as VPN users in AD server mapped to a realm. Also, you can select and use the domain computers as VPN users when creating access control rules or selecting the members of a community.

To select a domain computer as VPN users:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Select the **Mapped Accounts** tab.
3. Click + icon and select **Browse Directory** from the drop-down menu.
4. Select the **Realm** you want to search and select the **Folder**.

   Browse directory now allows browsing of both domain users and domain computers.



Realm: LDAP + RSA

Search directory: * Users & groups

Folders: LDAP + RSA

- □ win2012.com (11)
  - □ Builtin
  - □ Computers
  - □ Defender (5)
  - □ Domain Controllers
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Parent_OU (1)
  - □ shamnas_container
  - □ shamnas_OU
  - □ Test_OU
  - □ Users

Members: Computers (16)

- □ AVENTAIL$
- □ BLR1-CHANDRA-WI
- □ EX2K13
- □ EXCHG2013
- □ KF-DEVMACHINE-1$
- □ LTP08$
- □ OWA2013
- □ SALINI
- □ SCCMCLIENT02
- □ SHRPOINT2013
- □ VISTA-23$
- □ VISTA64-28$
- □ W8PRO-PC1
- □ WIN12
- □ WINDOWS7
- □ WINDOWSXP$

☑ Display 500 items in search results

Details: Computers

Name:
Computers
Username:
null
Domain:
win2012.com
Distinguished name:
CN=Computers,DC=win2012,DC=com
Description:
Default container for upgraded computer accounts
Member of:
(None)

Show attributes as: Summary

Managing Local User Accounts

Create local user accounts on the appliance in one of these ways:

- Manually create local user accounts in AMC and store them in a local user authentication repository.
- Import local user accounts from a comma-separated (CSV) text file and store them in a local user authentication repository. See Importing New Local Users and Groups.

Regardless of the method you use, local users are stored on the appliance, unlike all other users who are stored in external authentication repositories and referenced by AMC. AMC lets you create, modify, and delete local accounts for individual users on the appliance, and also supports local accounts for groups of users.

Topics:

- Adding Local Users
- Editing Local Users
- Deleting Local Users
- Adding Local Groups
- Editing Local Groups
- Deleting Local Groups

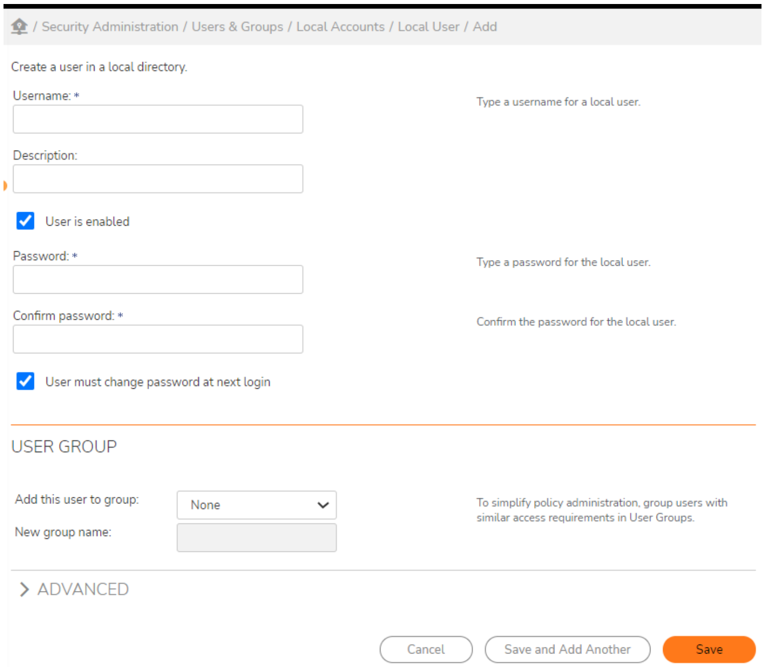
Adding Local Users

Before you can add local users, you must first create a local user authentication repository on the appliance, as described in Configuring Local User Storage. You do not need to configure a local authentication realm before adding local users.

After you've created a local user authentication repository, you can add local users to the appliance.

To add local users to the appliance:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Click the **+** (New) icon.
4. Select **User** from the drop-down list.



/ Security Administration / Users & Groups / Local Accounts / Local User / Add

Create a user in a local directory.

Username: * — Type a username for a local user.

Description:

☑ User is enabled

Password: * — Type a password for the local user.

Confirm password: * — Confirm the password for the local user.

☑ User must change password at next login

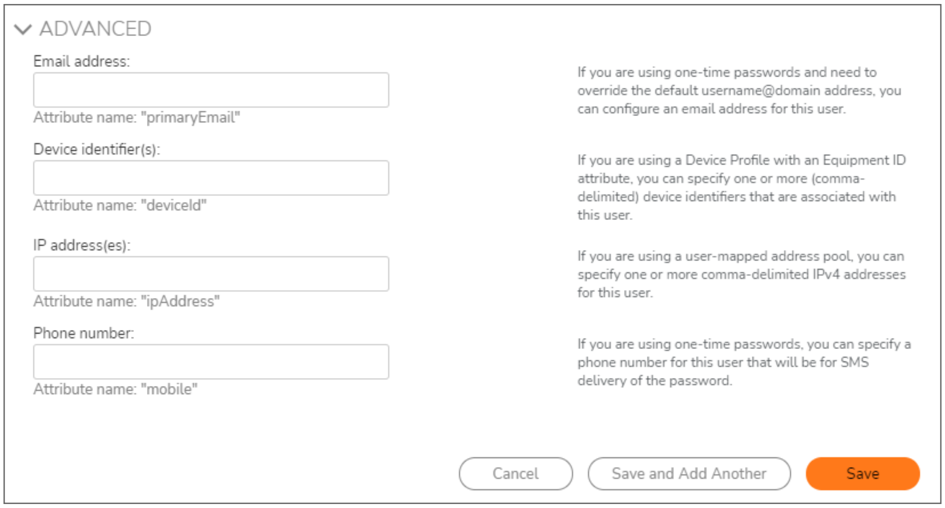
USER GROUP

Add this user to group: None — To simplify policy administration, group users with similar access requirements in User Groups.

New group name:

5. In the **Username** field, type the name of the local user you want to add to the local user authentication repository. The user name can be any length between 1 and 255 characters.
6. In the **Description** field, type a descriptive comment about the local user.
7. To enable the user to log in, select the **User is enabled** checkbox.
8. In the **Password** field, type a password for the local user, and type it again in the **Confirm Password** field.

   The password must conform to the password policy configured for the local authentication server. For more information, see Configuring Local User Storage.
9. To require the user to change password at initial login, select the **User must change password at next login** checkbox.
10. In the **User Group** section, select a local group for the user from the **Add this user to group** drop-down menu. Select:
    - **None** if you do not want to add the user to a local group.
    - **(New)** to create a new group for this user; and then enter the group name in the **New group name** field.
11. Expand the **Advanced** section to add an email address or device identifier for the user.



ADVANCED

Email address:

Attribute name: "primaryEmail"

If you are using one-time passwords and need to override the default username@domain address, you can configure an email address for this user.

Device identifier(s):

Attribute name: "deviceId"

If you are using a Device Profile with an Equipment ID attribute, you can specify one or more (comma-delimited) device identifiers that are associated with this user.

IP address(es):

Attribute name: "ipAddress"

If you are using a user-mapped address pool, you can specify one or more comma-delimited IPv4 addresses for this user.

Phone number:

Attribute name: "mobile"

If you are using one-time passwords, you can specify a phone number for this user that will be for SMS delivery of the password.

12. In the **Email Address** field, configure an email address for the user.

    This address is used for sending one-time passwords to the user, and overrides the default `username@domain` email address. This e-mail address is assigned to the **mail** attribute for the user.
13. In the **Device identifier(s)** field, enter one or more comma-delimited device identifiers for computers or other devices associated with this user. This value is used by the equipment identifier end-point-control feature to enforce user-device affinity. These values are assigned to the **deviceId** attribute.
14. In the **IP address(es)** field, enter one ore more comma-delimited IPv4 addresses for this user.
15. In the **Phone number** field, enter a phone number for this user that will be for SMS delivery of the password.
16. Click:

- **Save** to create the local user account and save it to the local user authentication repository on the appliance.
- **Save and Add Another** to save it and then configure another local user.

Editing Local Users

To change a local user's settings:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Click the name of the user you want to edit.

   The **Edit Local User** page displays.
4. Make any edits to the user's settings, and then click **Save**.

Deleting Local Users

ⓘ **IMPORTANT:** You cannot delete a local user if he or she is referenced by another object. See Deleting Referenced Objects for more details.

To delete a local user:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Select the checkbox for the user you want to delete.
4. Click the **X** (Delete) icon.

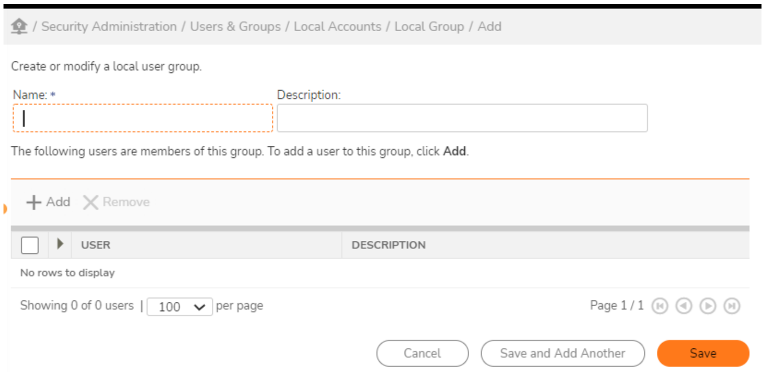
Adding Local Groups

Before you can add local groups, you must first create a local user authentication repository on the appliance, as described in Configuring Local User Storage. You do not need to configure a local authentication realm before adding local groups.

After you've created a local user authentication repository, you can add local groups to the appliance. Either add local groups manually or import groups, as explained in Importing and Exporting Local Accounts.

To add local groups to the appliance:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Click the **+** (New) icon.
4. Select **Group** from the drop-down list.



/ Security Administration / Users & Groups / Local Accounts / Local Group / Add

Create or modify a local user group.

Name: *

Description:

The following users are members of this group. To add a user to this group, click **Add**.

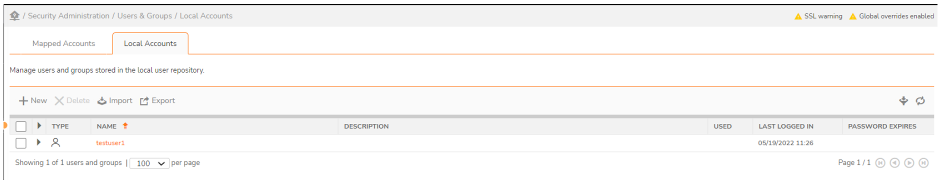
□	USER	DESCRIPTION

No rows to display

Showing 0 of 0 users | 100 per page

Page 1 / 1

5. In the **Name** field, type the name of the local group you want to add to the local user authentication repository.
6. In the **Description** field, type a descriptive comment about the local group.
7. To add a user to the group, click the **+** (New) icon.



/ Security Administration / Users & Groups / Local Accounts

SSL warning Global overrides enabled

Manage users and groups stored in the local user repository.

□	TYPE	NAME	DESCRIPTION	USED	LAST LOGGED IN	PASSWORD EXPIRES
□		testuser1			05/19/2022 11:26	

Showing 1 of 1 users and groups | 100 per page

Page 1 / 1

8. Select the checkbox beside each user you want to add to the group.
9. Click the **+** (New) icon.

   Only users who are not already in the selected group are displayed.
10. To create a new user, the **+** (New) icon to display the **Add User** page. See Adding Local Users for a description of the fields.
11. Click:
    - **Save** to create the local user group and save it to the local user authentication repository on the appliance.
    - **Save and Add Another** to save it and then configure another local group.

Editing Local Groups

To change a local group's settings:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Click the name of the group you want to edit.

   The **Edit Local Group** page displays.
4. Make any edits to the group's settings.
5. Click **Save**.

Deleting Local Groups

ⓘ **IMPORTANT:** You cannot delete a local group if it is referenced by another object. See Deleting Referenced Objects for more details.

To delete a local group:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Select the groups you want to delete.
4. Click the **X** (Delete) icon.

Importing and Exporting Local Accounts

SMA appliances use CSV files to import and export user and group information. User and group information can be imported for new and existing user accounts as long as the CSV file conforms to the guidelines shown in Creating the CSV File. Detailed import information is provided in Importing New Local Users and Groups and Importing Data for Existing Local Users.

Export creates a CSV file named `LocalUsers.csv` that contains all local user accounts in the local user authentication repository. Follow the guidelines in Exporting Local User Accounts to create the export file.

Topics:

- Importing New Local Users and Groups
- Importing Data for Existing Local Users
- Importing New Groups
- Exporting Local User Accounts
- Import and Export Error Messages

Importing New Local Users and Groups

To easily add or edit local users and groups, import local user information from a comma-separated (CSV) text file into the appliance configuration. This time-saving feature is especially useful to new customers who must add numerous local users to the appliance. Importing users is also very useful when you need to update one or more properties for existing users. For example, you can quickly add a new group to several users when a new group is created. See Importing Data for Existing Local Users for additional information.

Before you can import local users and groups, you must first create a local user authentication repository on the appliance, as described in Configuring Local User Storage. Once you've created a local user authentication repository, you can import local users and groups to the appliance.

ⓘ **NOTE:** A local authentication realm does not need to be created before importing local users and groups.

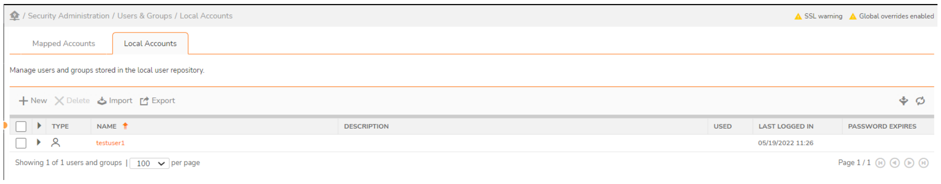
To import local users and groups to the appliance:

1. Ensure the CSV file to be imported resides on the local computer and adheres to the guidelines mentioned in Creating the CSV File.

   ⓘ | **IMPORTANT:** No data is imported if AMC encounters any errors in the CSV file.

2. In the AMC, navigate to **Security Administration > Users & Groups**.

3. Click the **Local Accounts** tab.

   / Security Administration / Users & Groups / Local Accounts

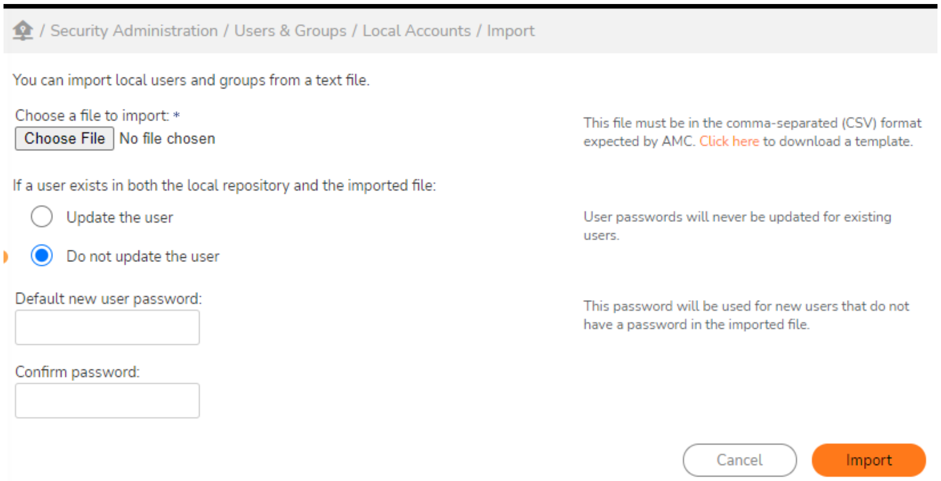
   Manage users and groups stored in the local user repository.

□		TYPE	NAME	DESCRIPTION	USED	LAST LOGGED IN	PASSWORD EXPIRES
□			testuser1			05/19/2022 11:26	

   Showing 1 of 1 users and groups | 100 per page

   Page 1 / 1

   Click the **Import** button, which displays the **Import Local Users** page you use to import local users from a CSV file into the local user authentication repository.

   / Security Administration / Users & Groups / Local Accounts / Import

   You can import local users and groups from a text file.

   Choose a file to import: *

   Choose File No file chosen

   This file must be in the comma-separated (CSV) format expected by AMC. Click here to download a template.

   If a user exists in both the local repository and the imported file:

   ○ Update the user

   ● Do not update the user

   User passwords will never be updated for existing users.

   Default new user password:

   This password will be used for new users that do not have a password in the imported file.

   Confirm password:

   You must have modify access to the **Local Accounts** page and a local user authentication repository must be available.

4. In the **Choose a file to import** field, click **Browse** to locate the file you want to import. Before importing a file, ensure that it meets the requirements shown in Creating the CSV File.

5. Select how a user account that is in both the local user authentication repository and the imported file should be handled:

Select	To
Update the User	Update the duplicate user data in the local user authentication repository to match the user record in the imported CSV file
Do not update the user	Ignore the duplicate user record in the CSV file and leave the user data in the local user authentication repository unchanged

   Regardless of this setting, the passwords of existing users are never updated. However, passwords for new users are imported.

6. In the **Default new user password** field, type the password to be used by all new imported local users who do not have a password defined in the CSV file. The password must conform to the password policy configured for the local authentication server. New users will use this default password to login the first time.
7. Retype the default password in the **Confirm password** field.
8. Click the **Import** button to add local user accounts to the local user authentication repository.

Creating the CSV File

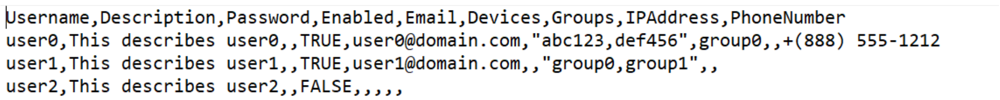
The CSV file used to import user accounts into the appliance must be generated with the guidelines shown in the below table, and fields must be in the order shown.

CSV File Field Order

Field	Required or Optional	Guidelines	Description
Username	Required	1-255 characters (case-sensitive)	Name the user enters to login
Description	Optional	Any number and type of characters allowed	Additional information about the user
Password	Optional	Must conform to the password policy configured for the local authentication server (used only when importing new users)	Password the user enters to login
Enabled	Required	Must contain either `True`or `False` ⓘ | **NOTE:** Case-sensitive	Whether the user is allowed to login
E-mail	Optional	Local user name and domain name separated by an `@` (up to 254 characters)	Valid e-mail address used to send one-time passwords to the user
Devices	Optional	Comma-separated list	Device IDs associated with the user
Groups	Optional	Comma-separated list (up to 255 characters) ⓘ | **NOTE:** A group is created if AMC tries to import an undefined group.	Comma-separated list of groups to which the user belongs

IPAddress	Optional	Single IPv4 address, each IPv4 address should match the network address of the resource interface. List of IPv4 addresses, these addresses are presented to the User-Mapped Tunnel Address Pool, in the order they appear in the list.	If you are using a user-mapped address pool, you can specify one or more comma-delimited IPv4 addresses for this user.
Phone number	Optional	mobile number	Phone number associated with the user that receives one-time password SMS

This example shows the file format required to import users into AMC:



```
Username,Description,Password,Enabled,Email,Devices,Groups,IPAddress,PhoneNumber
user0,This describes user0,,TRUE,user0@domain.com,"abc123,def456",group0,,+(888) 555-1212
user1,This describes user1,,TRUE,user1@domain.com,,"group0,group1",,
user2,This describes user2,,FALSE,,,,,
```

The following guidelines are also required, as shown in the above example:

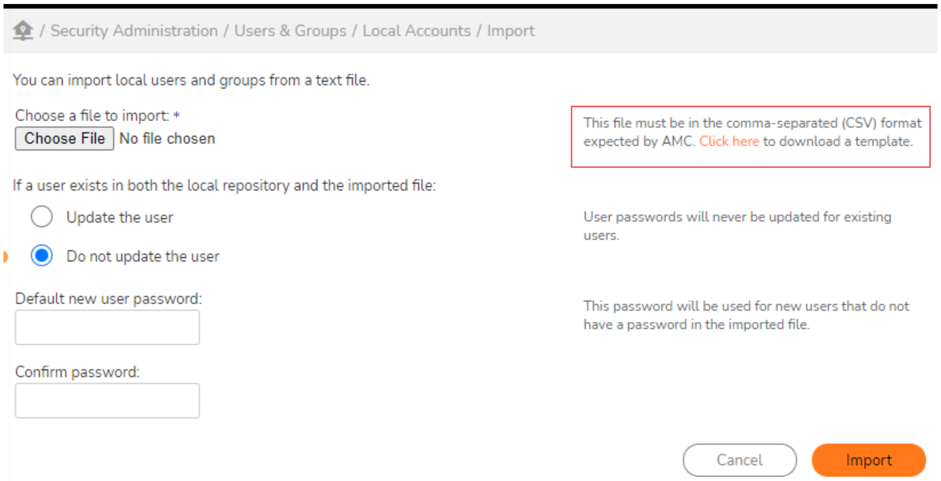
- The first row of the file is ignored, because the CSV format uses the first row as column headers.
- String values are typically quoted using double quotes (“).
- String values containing commas must be quoted.
- String values containing quotes must escape the quote by using another double quote character, for example, “`The group name is` “”`Team1`””.”

If AMC encounters any errors in the CSV file, no data is imported and an error message is displayed. Error messages are shown in Import and Export Error Messages.

Downloading a CSV Template

To download a template you can use to create the CSV file containing user data:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.
3. Click the **Import** button.
4. On the **Import Local Users** page, click the **Click here** link



/ Security Administration / Users & Groups / Local Accounts / Import

You can import local users and groups from a text file.

Choose a file to import: *

No file chosen

This file must be in the comma-separated (CSV) format expected by AMC. Click here to download a template.

If a user exists in both the local repository and the imported file:

○ Update the user

● Do not update the user

User passwords will never be updated for existing users.

Default new user password:

This password will be used for new users that do not have a password in the imported file.

Confirm password:

5. When the Windows **File Download** page displays, click the **Save** button.
6. When the Windows Save As page displays, either:
   - Click the **Save** button to accept the defaults. By default, the file is named `LocalUsersTemplate.csv` and located in your Downloads folder.
   - Select another file name and location for the CSV file.
7. After downloading the file, use it as a guide to add user data that you want to import into the local user authentication repository.

Importing Data for Existing Local Users

As an alternative to manually editing user accounts, import users when you need to update one or more properties for several user accounts already in the local user authentication repository. For example, you can quickly add several users to a group when a new group is created. Simply export user accounts to a CSV file, change the desired properties, and then import the revised user accounts back into the local user authentication repository.

To import data for existing local users, follow the instructions in Importing New Local Users and Groups with the following exceptions:

- When selecting whether data should be updated for the user, be sure to select **Update the User**.

  Passwords are imported for new users only. Regardless of this setting, the passwords of existing users are never updated.
- Use the same CSV file format used to import new users. See Creating the CSV File. However, only the following properties are imported.
  - Description
  - E-mail Address
  - Device IDs
  - Groups
- Properties can be added but not removed when importing users.

Importing New Groups

When importing data for new or existing local users, group memberships also are imported (if available in the imported CSV file). AMC does not explicitly import local groups. However, if a user is a member of a group that has not been configured in AMC, a new local group is created and the user is added as a member of the group.

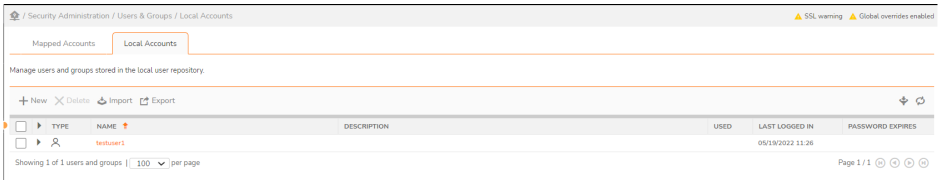
△ **CAUTION: Make sure all group names in the CSV file are correct. Otherwise, unwanted groups will be created.**

Exporting Local User Accounts

The AMC provides the ability to create a CSV-formatted text file by exporting local user accounts and related group information currently defined in the local user authentication repository. This CSV file can then be used to import user data into any database.

To export local user accounts:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click the **Local Accounts** tab.



/ Security Administration / Users & Groups / Local Accounts

SSL warning Global overrides enabled

Manage users and groups stored in the local user repository.

TYPE	NAME	DESCRIPTION	USED	LAST LOGGED IN	PASSWORD EXPIRES
	testuser1			05/19/2022 11:26	

Showing 1 of 1 users and groups | 100 per page

Page 1 / 1

3. Click the **Export** button, which displays the **Windows File Download** .
4. Click the **Save** button.
5. When the **Windows Save As** page displays, either:
   - Click the **Save** button to accept the defaults. By default, the file is named `LocalUsers.csv` and located in your Downloads folder.
   - Select another file name and location for the CSV file.

Import and Export Error Messages

The following error messages may occur when importing or exporting a CSV file. If an error is encountered during import, no data is imported. Therefore, you must correct the error before the file can be imported.

`Duplicate user names`	If the same user name (case-insensitive) appears in more than one record in the CSV file, an error message identifies the user name and line on which the duplicate user name appears.
`Wrong number of data columns`	If a record contains an invalid number of columns, an error message indicates that the data is invalid and identifies the line number of the record.

`Invalid email address`	If a record contains an e-mail address that is not a valid address (for example "`useratdomain.com`"), an error message identifies the user name, invalid address, and line number where the invalid address occurs.
`Invalid default password`	If the default password does not meet the password criteria configured on the local authentication server, an error message identifies the criteria that is not met. For example, if the password does not contain either an uppercase letter or a symbol but is required to have at least one or both, the error message indicates that both are missing.
`Invalid "enabled" value`	If the value for the Enabled column is not "`true`" or "`false`", an error message identifies the problem and line number of the record.
`Invalid user name`	If a user name is invalid (for example, more than 255 characters), an error message identifies the problem and line number of the record.
`Invalid group name`	If a group name is invalid (for example, more than 255 characters), an error message identifies the problem and line number of the record.
`Missing user name`	If an entry is missing a user name, an error message identifies the problem and line number of the record.
`Missing password` (and no default provided for new users)	If an entry for a new user is missing a password and no default password is provided, an error message identifies the problem and line number of the record.
`Invalid user password`	If an entry for a new user contains a password that does not meet the password policy configured on the local authentication server, an error message identifies that the password does not meet the policy and the line number of the problem.

Integrating an SMA Appliance with a SonicWall Firewall

Secure Mobile Access (SMA) 1000 series appliances running firmware version 12.4 and higher can be integrated to work with SonicWall TZ,NSv, NSsp, NSA, and SuperMassive series firewalls running firmware version SonicOS 6.5.4 and higher.

These devices can be integrated to share session information using the SonicOS Single Sign-On (SSO) feature. The SonicWall TZ, NSv, NSsp, NSA, and SuperMassive series firewall can be configured to act as a RADIUS accounting server and to receive RADIUS accounting records from a Secure Mobile Access (SMA) 1000 series appliance.

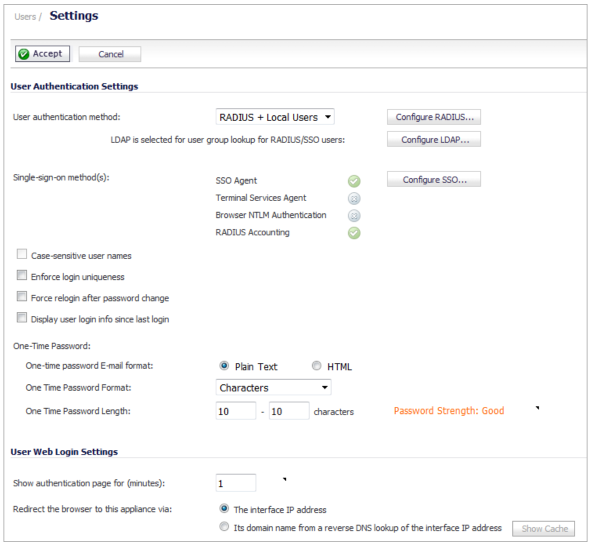
Topics:

- Configuring a Firewall to Receive RADIUS Accounting Records from an SMA Appliance
- Configuring an SMA Appliance to Send RADIUS Accounting Records to a Firewall
- Viewing SMA Users on the Firewall

Configuring a Firewall to Receive RADIUS Accounting Records from an SMA Appliance

To configure a firewall to receive RADIUS accounting records from an SMA Appliance:

1. On the firewall, go to the **Users > Settings** page.



Users / **Settings**

User Authentication Settings

User authentication method: RADIUS + Local Users

LDAP is selected for user group lookup for RADIUS/SSO users:

Single-sign-on method(s):
SSO Agent ✓
Terminal Services Agent ⊗
Browser NTLM Authentication ⊗
RADIUS Accounting ✓

□ Case-sensitive user names
□ Enforce login uniqueness
□ Force relogin after password change
□ Display user login info since last login

One-Time Password:

One-time password E-mail format: ● Plain Text ○ HTML

One Time Password Format: Characters

One Time Password Length: 10 - 10 characters Password Strength: Good

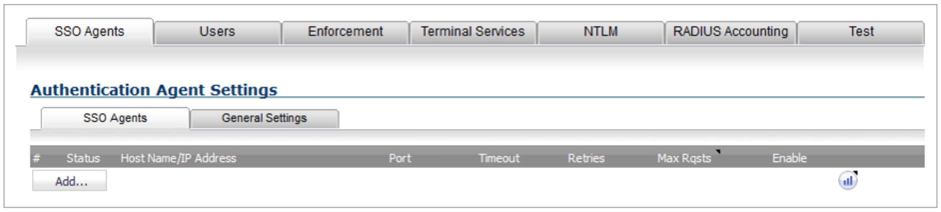
User Web Login Settings

Show authentication page for (minutes): 1

Redirect the browser to this appliance via:
● The interface IP address
○ Its domain name from a reverse DNS lookup of the interface IP address

2. Click **Configure SSO**.

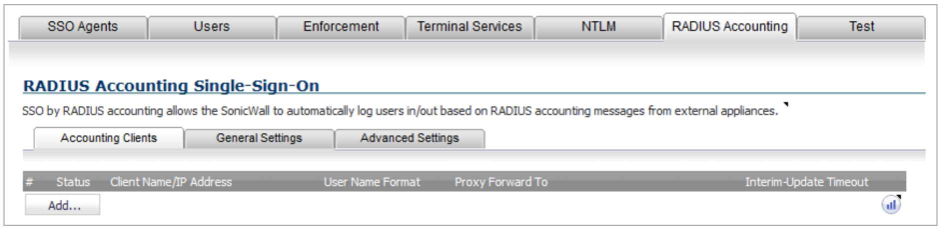
   The **SonicWall SSO Authentication Configuration** page displays.



Authentication Agent Settings

#	Status	Host Name/IP Address	Port	Timeout	Retries	Max Rqsts	Enable

3. Select the **RADIUS Accounting** tab.



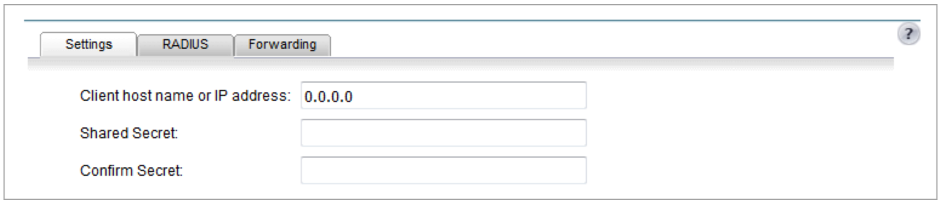
RADIUS Accounting Single-Sign-On

SSO by RADIUS accounting allows the SonicWall to automatically log users in/out based on RADIUS accounting messages from external appliances.

#	Status	Client Name/IP Address	User Name Format	Proxy Forward To	Interim-Update Timeout

4. Select the **Accounting Clients** tab.
5. Click **Add**.

   The **Settings** tab appears.



Client host name or IP address: 0.0.0.0

Shared Secret:

Confirm Secret:

6. In the **Client host name or IP address** field, enter the IP address or host name of the internal interface on the SMA appliance (RADIUS client) that is connected to the firewall (RADIUS server).

7. Enter the **Shared Secret**.

   > ⓘ **NOTE:** The **Shared Secret** is a text string of your choice that serves as the password between the RADIUS client and the RADIUS server. This instance of the **Shared Secret** is for the firewall, which is acting as the RADIUS server. You will enter this same **Shared Secret** when you configure the SMA appliance.

8. Enter the **Shared Secret** again in the **Confirm Secret** field.

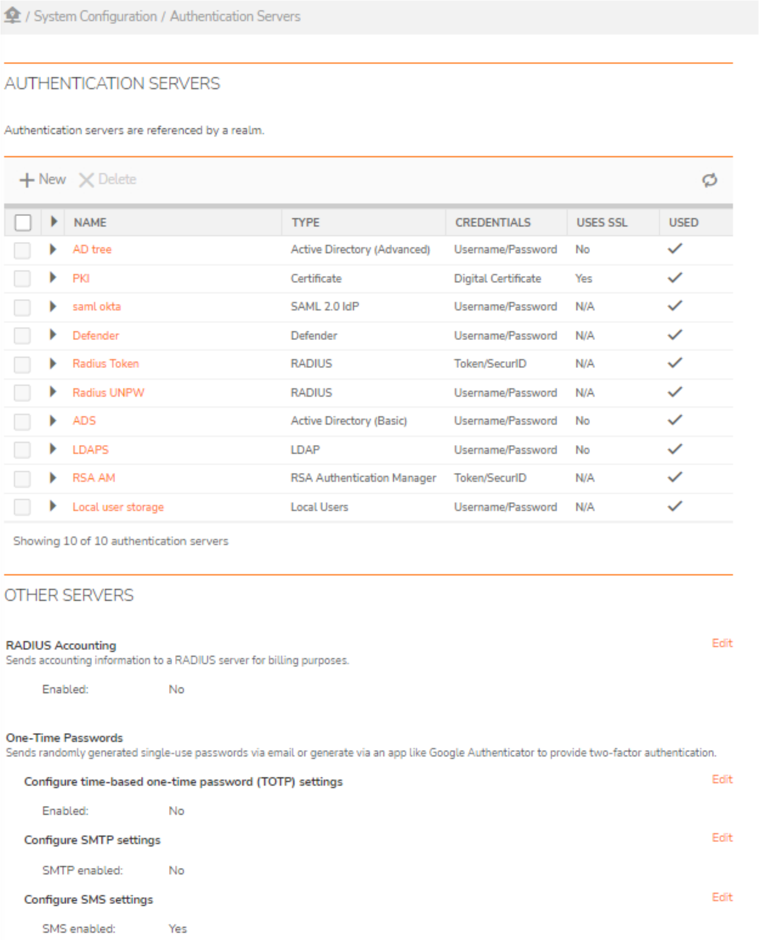
9. Click **Apply**.

10. Click **OK**.

Configuring an SMA Appliance to Send RADIUS Accounting Records to a Firewall

To configure an SMA appliance to send RADIUS accounting records to a firewall:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

☐	NAME	TYPE	CREDENTIALS	USES SSL	USED
☐	AD tree	Active Directory (Advanced)	Username/Password	No	✓
☐	PKI	Certificate	Digital Certificate	Yes	✓
☐	saml okta	SAML 2.0 IdP	Username/Password	N/A	✓
☐	Defender	Defender	Username/Password	N/A	✓
☐	Radius Token	RADIUS	Token/SecurID	N/A	✓
☐	Radius UNPW	RADIUS	Username/Password	N/A	✓
☐	ADS	Active Directory (Basic)	Username/Password	No	✓
☐	LDAPS	LDAP	Username/Password	No	✓
☐	RSA AM	RSA Authentication Manager	Token/SecurID	N/A	✓
☐	Local user storage	Local Users	Username/Password	N/A	✓

Showing 10 of 10 authentication servers

OTHER SERVERS

RADIUS Accounting Edit
Sends accounting information to a RADIUS server for billing purposes.

Enabled: No

One-Time Passwords
Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings Edit

Enabled: No

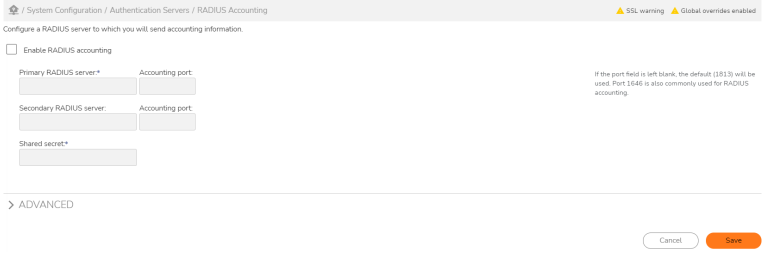
Configure SMTP settings Edit

SMTP enabled: No

Configure SMS settings Edit

SMS enabled: Yes

2. Under **Other servers**, click the **Edit** icon for **RADIUS Accounting**.



/ System Configuration / Authentication Servers / RADIUS Accounting

Configure a RADIUS server to which you will send accounting information.

☐ Enable RADIUS accounting

Primary RADIUS server:* Accounting port:

Secondary RADIUS server: Accounting port:

Shared secret:*

If the port field is left blank, the default (1813) will be used. Port 1646 is also commonly used for RADIUS accounting.

3. Select the **Enable RADIUS Accounting** checkbox.

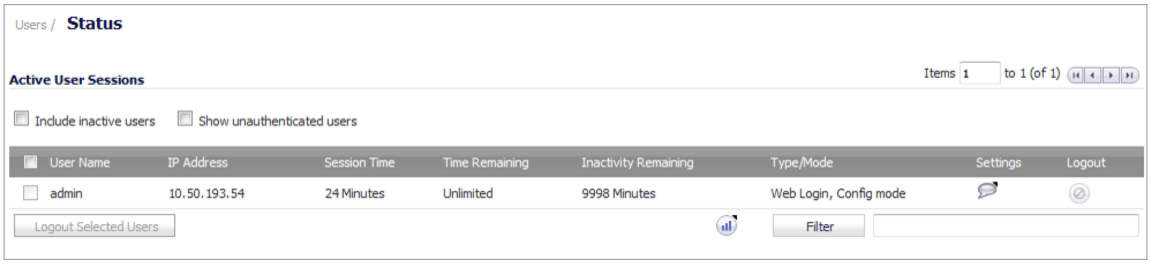
4. In the **Primary RADIUS server** field, enter the IP address of the firewall that you configured in Integrating an SMA Appliance with a SonicWall Firewall.
    a. In the **Accounting port** field, enter the port number you want to use. If the port field is left blank, the default port (**1813**) is used. Port 1646 is also commonly used for RADIUS accounting.
5. In the **Secondary RADIUS server** field, enter the IP address of the firewall that you configured in Integrating an SMA Appliance with a SonicWall Firewall.
    a. In the **Accounting port** field, enter the port number you want to use. If the port field is left blank, the default port (**1813**) is used. Port 1646 is also commonly used for RADIUS accounting.
6. In the **Shared secret** field, enter the same **Shared Secret** you configured on the firewall in Integrating an SMA Appliance with a SonicWall Firewall.
7. Click **Save**.

Viewing SMA Users on the Firewall

When your SonicWall firewall is connected to an SMA appliance via a VPN client, you can view the SMA users on the firewall.

To view SMA users on the firewall:

1. On the firewall, go to the **Users > Status** page.



Users / **Status**

Active User Sessions

Items 1 to 1 (of 1)

☐ Include inactive users ☐ Show unauthenticated users

☐	User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining	Type/Mode	Settings	Logout
☐	admin	10.50.193.54	24 Minutes	Unlimited	9998 Minutes	Web Login, Config mode		⊘

Logout Selected Users

Filter

2. Select the checkbox for **Include inactive users**.

   SMA users should appear in the list.

   As the SMA users are logged into a device that is external to the firewall, the firewall treats those user sessions as inactive. To see the SMA users displayed on this page, you must select the checkbox for **Include inactive users**. After the firewall is configured to receive RADIUS accounting information from the SMA appliance, users are automatically added to this list as soon as they are successfully authenticated by the SMA appliance. They are removed automatically when their SMA session ends.

4

Authentication

Topics:

Network and Authentication Configuration

Topics:

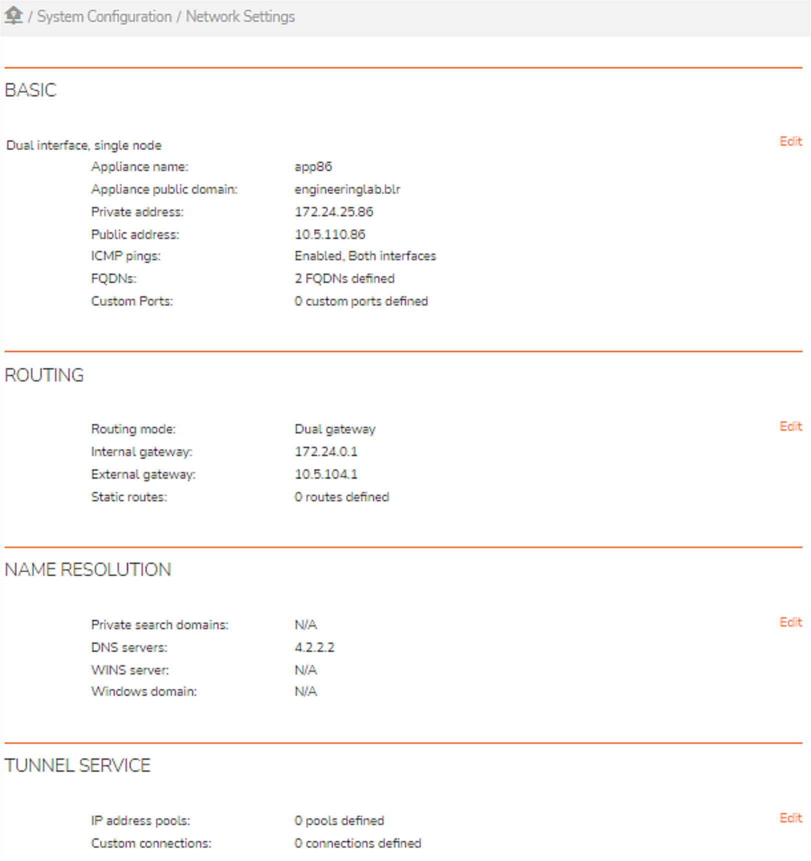
About Configuring the Network

This section provides information about essential network configuration tasks, including configuring network interfaces, selecting a routing mode, configuring network gateways, defining static routes, and name resolution. It also explains how to manage SSL and CA certificates, and configure user authentication.

This is the minimal network configuration required to get the appliance up and running. For information on configuring additional services—including NTP, SSH, ICMP, and syslog—see System Administration.

Configuring Basic Network Settings

All basic network settings—including IP interfaces, routing, and name resolution—are configurable in AMC. The starting point in AMC for configuring network options is the **System Configuration > Network Settings** page.



/ System Configuration / Network Settings

BASIC

Dual interface, single node

Edit

Appliance name:	app86
Appliance public domain:	engineeringlab.blr
Private address:	172.24.25.86
Public address:	10.5.110.86
ICMP pings:	Enabled, Both interfaces
FQDNs:	2 FQDNs defined
Custom Ports:	0 custom ports defined

ROUTING

Edit

Routing mode:	Dual gateway
Internal gateway:	172.24.0.1
External gateway:	10.5.104.1
Static routes:	0 routes defined

NAME RESOLUTION

Edit

Private search domains:	N/A
DNS servers:	4.2.2.2
WINS server:	N/A
Windows domain:	N/A

TUNNEL SERVICE

Edit

IP address pools:	0 pools defined
Custom connections:	0 connections defined

Topics:

- Specifying System Identity
- Configuring Network Interfaces
- Configuring ICMP
- Viewing Fully Qualified Domain Names and Custom Ports

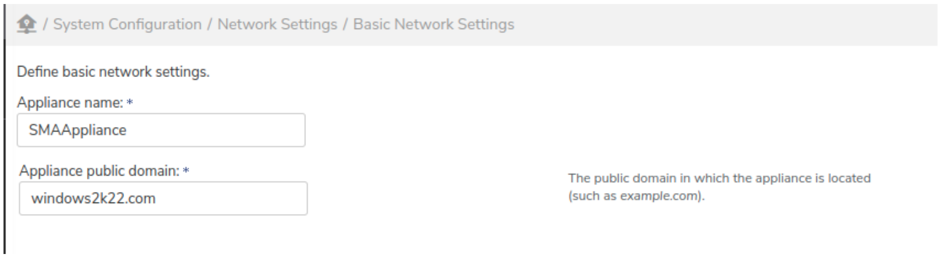
Specifying System Identity

You must name the appliance and specify the domain name in which it is located.

To specify system identity:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Basic** section, click **Edit**.

   The **Basic Network Settings** page displays.



/ System Configuration / Network Settings / Basic Network Settings

Define basic network settings.

Appliance name: *
SMAAppliance

Appliance public domain: *
windows2k22.com

The public domain in which the appliance is located (such as example.com).

3. The **Appliance name** is the host name that is set in CMS on the **Managed Appliances** page.

   The **Appliance name** helps you differentiate appliances in several contexts (especially if more than one appliance is running):

   - It sets the command prompt for the SMA appliance.
   - It is saved to a log file, so you can identify the appliance to which a particular log message applies.
   - When you export a configuration file for the appliance (on the **Maintenance** page in AMC), the **Appliance name** is prepended to the file name.

   The name is not visible to users.

4. In the **Appliance public domain** field, type the name of the domain in which the appliance is located (for example, `yourcompany.com`). This name defines the DNS namespace used to identify hosts accessed by the appliance.

Configuring Network Interfaces

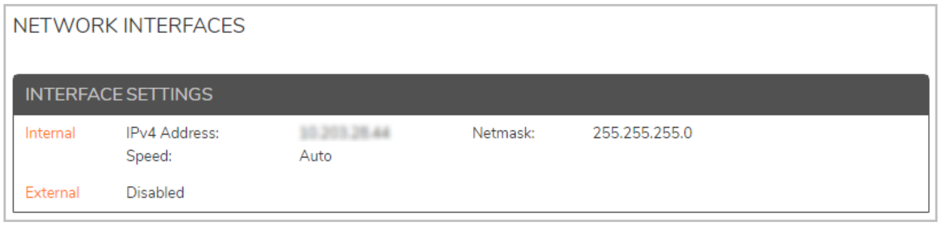
To configure the network interfaces, specify the IP address, subnet mask, and interface speed. You can run the appliance using both the internal and the external interfaces (a dual-homed configuration), or optionally just the internal interface (a single-homed configuration). For more information on the interface configuration options, see Network Architecture.

To configure network interfaces:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Basic** section, click **Edit**.

   The **Basic Network Settings** page displays.

3. In the **Network interfaces** area, configure the settings for the internal interface connected to your internal (or private) network.



NETWORK INTERFACES

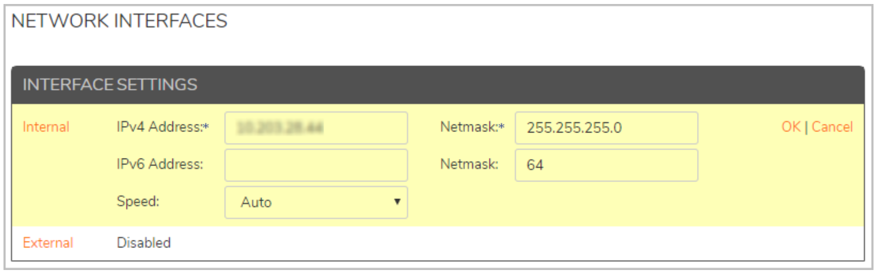
INTERFACE SETTINGS

Internal IPv4 Address: [redacted] Netmask: 255.255.255.0
Speed: Auto

External Disabled

a. Click **Internal**.

   The display becomes editable.



NETWORK INTERFACES

INTERFACE SETTINGS

Internal IPv4 Address:* [redacted] Netmask:* 255.255.255.0 OK | Cancel
IPv6 Address: Netmask: 64
Speed: Auto ▾

External Disabled

b. Type an **IPv4 Address** and **Netmask** for the interface.

   - Optionally you can enter the **IPv6 Address** and **Netmask**

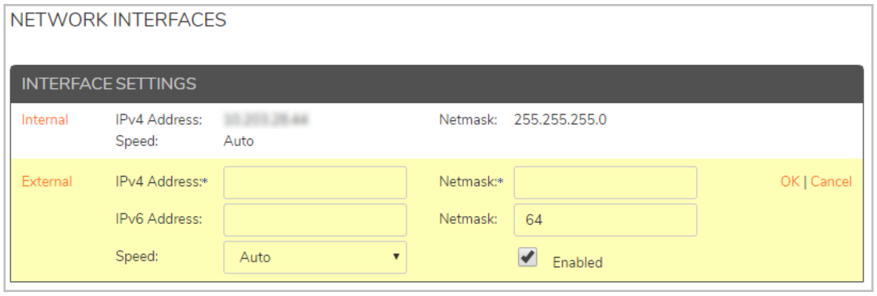
c. Select the appropriate **interface Speed** from the list (the default is **Auto**).

d. Click **OK**.

4. Configure the settings for the interface connected to the external network (or Internet):

a. Click **External**.

   The display becomes editable.



NETWORK INTERFACES

INTERFACE SETTINGS

Internal IPv4 Address: [redacted] Netmask: 255.255.255.0
Speed: Auto

External IPv4 Address:* Netmask:* OK | Cancel
IPv6 Address: Netmask: 64
Speed: Auto ▾ ☑ Enabled

b. Type the **Address** and **Netmask** settings used to access the SMA appliance from the Internet.

   The external IPv4 or IPv6 address must be publicly accessible.

c. Select the appropriate **interface Speed** from the list (the default is **Auto**).

d. Select the **Enabled** checkbox.

e. Click **OK**.

5. Click **Save**.

6. Click **Pending changes**.

7. Apply the changes. (For more information, see Applying Configuration Changes.)

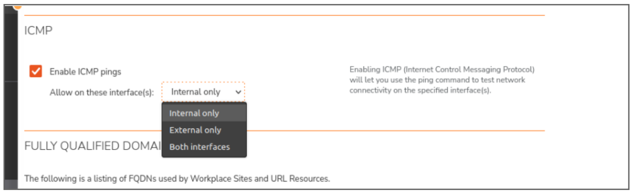
If you configure the appliance to use both the internal and external interfaces, verify your routing settings to make sure that you have a network route to the internal interface. If the appliance is on a different network than the computer you're using to access AMC, you must set up routing (configure an internal default network gateway that will pass traffic to an internal router, or define a static route to the network on which the appliance is installed) to maintain access to AMC after you apply your network configuration changes. For more information, see Configuring Routing.

Configuring ICMP

Enabling ICMP (Internet Control Messaging Protocol) lets you use the ping command to test network connectivity on a IPv4 or IPv6 interface.

From 12.4.2 onwards in AMC/CMC you can select multiple interface option for ICMP for internal only or external only or both interfaces.

1. In the AMC, navigate to **System Configuration** > **Network Settings**.
2. In the **Basic** section, click the **Edit**.
   The **Basic Network Settings** page displays.
3. In the **ICMP** section, select the **Enable ICMP pings** checkbox.
4. In **Allow on these interface(s)**, select any of the following:
   - **Internal only**
   - **External only**
   - **Both Interfaces**



ICMP

☑ Enable ICMP pings

Allow on these interface(s): Internal only

Enabling ICMP (Internet Control Messaging Protocol) will let you use the ping command to test network connectivity on the specified interface(s).

FULLY QUALIFIED DOMAI

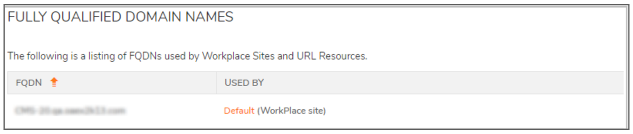
The following is a listing of FQDNs used by Workplace Sites and URL Resources.

5. Click **Save** and apply pending changes.

ⓘ **NOTE:** The CMS supports only the internal interface. Use other values when using policy synchronization to push ICMP configuration to managed appliances.

Viewing Fully Qualified Domain Names and Custom Ports

The **Fully qualified domain names** section of the page provides a table of the IPv4 or IPv6 addresses, FQDNs, and the WorkPlace sites and URL resources they are used by. You can sort the list forward or backward by any column heading by clicking the column heading link.



FULLY QUALIFIED DOMAIN NAMES

The following is a listing of FQDNs used by Workplace Sites and URL Resources.

FQDN	USED BY
[redacted]	Default (WorkPlace site)

Under **Used by**, click a WorkPlace site name or URL resource name that appears as a link to go to that page in AMC where you can edit the settings for it. The **Custom ports** section provides a table showing the custom port number and the URL resource that uses that port for all URL resources configured to use custom ports. Under **Used by resource**, click a URL resource name that appears as a link to go to the **Resources > Edit Resource** page to edit the resource settings.

Configuring Routing

The SMA appliance can be configured to route traffic using network gateways or static routes. These routing methods can be used separately or in combination with each other.

Topics:

- About Routing
- Configuring Network Gateways
- Choosing a Network Gateway Option
- Configuring Network Gateways in a Dual-Homed Environment
- Configuring Network Gateways in a Single-Homed Environment
- Enabling a Route to the Internet
- Configuring Static Routes

About Routing

- If you configure the appliance to use both the internal and external interfaces, verify the routing settings to make sure that you have a network route to the internal interface. If the appliance is on a different network than the computer you're using to access AMC, you must set up routing (configure an internal default network gateway that will pass traffic to an internal router, or define a static route to the network on which the appliance is installed) to maintain access to AMC after you apply your network configuration changes. For more information, see Configuring Routing.
- The routing information in AMC is sorted as follows:
  - The primary key is the **Netmask**, with entries sorted in descending order (from largest to smallest)
  - The secondary key is **IP address**, with entries sorted in ascending order (from smallest to largest)
- If your internal network has a contiguous address space, you can combine multiple static routes into one entry by specifying the proper subnet mask when you create the static route. The below table provides two examples of using a subnet mask to route internal traffic to multiple networks from a single static route entry:

Multiple Static Routes Combining

To route traffic to these networks:	Type this IP address	Type this subnet mask

`192.168.0.0`
`192.168.1.0`
`192.168.2.0`
`192.168.3.0`
	`192.168.0.0`	`255.255.252.0`

`192.168.*.*` (all networks in `192.168` range)	`192.168.0.0`	`255.255.0.0`

If necessary, you can explicitly create additional static routes for other subnets; the routing table searches net masks from most to least specific.

Configuring Network Gateways

A network gateway is the address of a router that serves as point of access to another network. Network gateway options are based on your network architecture and depend on whether you have configured the appliance as dual-homed (both internal and external interfaces are enabled) or single-homed (only the internal interface is enabled). See Network Architecture for more information.

Topics:

- Choosing a Network Gateway Option
- Configuring Network Gateways in a Dual-Homed Environment
- Configuring Network Gateways in a Single-Homed Environment

Choosing a Network Gateway Option

When configuring network gateways in a dual-homed environment, you can choose among four routing mode options:

- Dual gateway
- Single gateway, restricted
- Single gateway, unrestricted
- No gateway

Use these scenarios to help you decide which option is best for your needs:

- Scenario 1: Using an Internal and Internet Router
- Scenario 2: Managing Client Requests with Static Routes
- Scenario 3: Returning Client Requests to a Specified Gateway

- Scenario 4: Evaluating the Appliance in a Lab Setting
- Scenario 5: Deploying Network Tunnel Clients in “Redirect All” Mode

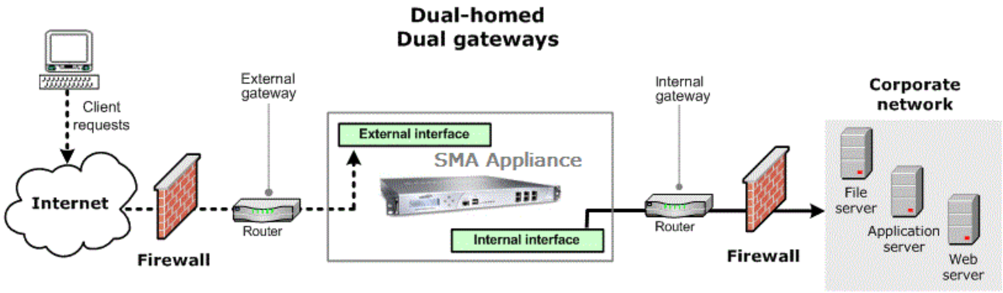
Scenario 1: Using an Internal and Internet Router

If you have an internal router as well as an Internet router, use the **Dual gateway** option. You can leverage your internal router to access your internal resources.

Sample Scenario

Company A has resources and a number of subnets on their internal network, and they already have a robust routing system in place. With the dual gateway routing mode on the appliance, client requests destined for internal resources on the corporate network can be delivered to an internal router. See the below image.

Internal And Internet Router Usage



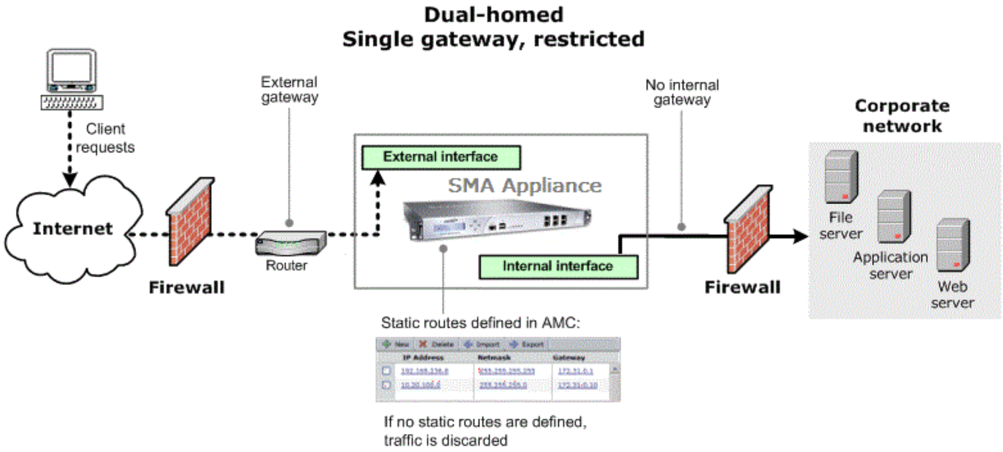
Scenario 2: Managing Client Requests with Static Routes

If you're not using an internal router, or prefer managing routing on the appliance, use the *Single gateway, restricted* option. In this scenario you must define static routes for all of your client requests. Client requests without a static route will be discarded by the appliance. This option requires more effort, but allows greater control over in-bound traffic.

Sample Scenario

Company B does not use a lot of internal resources, and prefers to manage its routing information on the appliance. They create a static route for each resource to which their VPN users should have access. If a VPN user attempts to reach an address that is not defined within the appliance's routing table, then the traffic is discarded. See the below image.

Managing Client Requests With Static Routes



	IP Address	Netmask	Gateway
□	192.168.236.0	255.255.255.255	172.21.0.1
□	10.20.100.0	255.255.255.0	172.21.0.20

Scenario 3: Returning Client Requests to a Specified Gateway

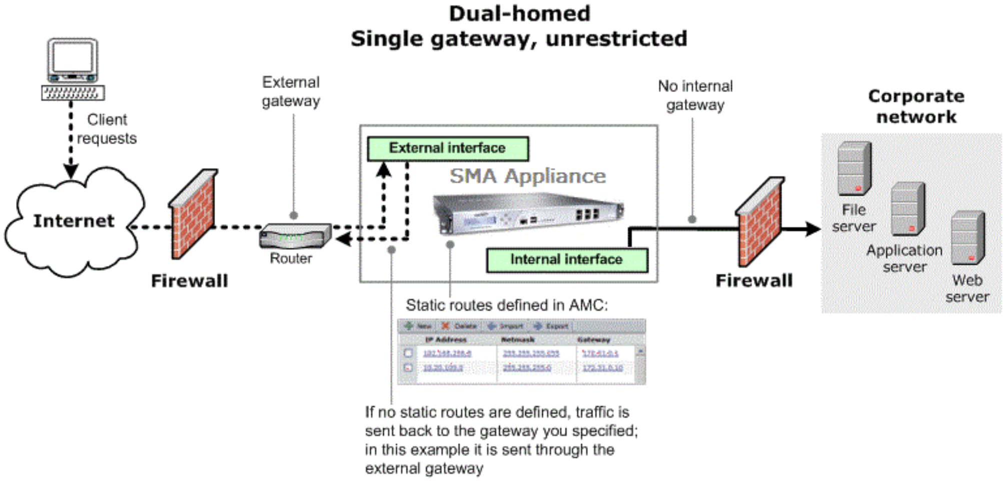
With the **Single gateway**, **unrestricted** option, the appliance delivers all client requests that do not match a static route to the gateway that you specify (on either the internal or external interface of the appliance). This option is less secure because it could allow traffic to pass to your Internet router and out of your network, depending on the filtering and routing policies of your infrastructure. This configuration is also more difficult to maintain.

Sample scenario

Like company B, company C prefers to manage its routing information on the appliance and has created static routes for each resource to which VPN users need access. However, some users in this organization also need access to Internet resources, and this traffic must be redirected from the appliance. For example, a company's users might need to access a public Web server that requires pre-registered IP addresses. See the below image.

A user must first establish a VPN session with the appliance; the request is then redirected to the external gateway of the appliance.

Returning Client Requests To A Specified Gateway



Scenario 4: Evaluating the Appliance in a Lab Setting

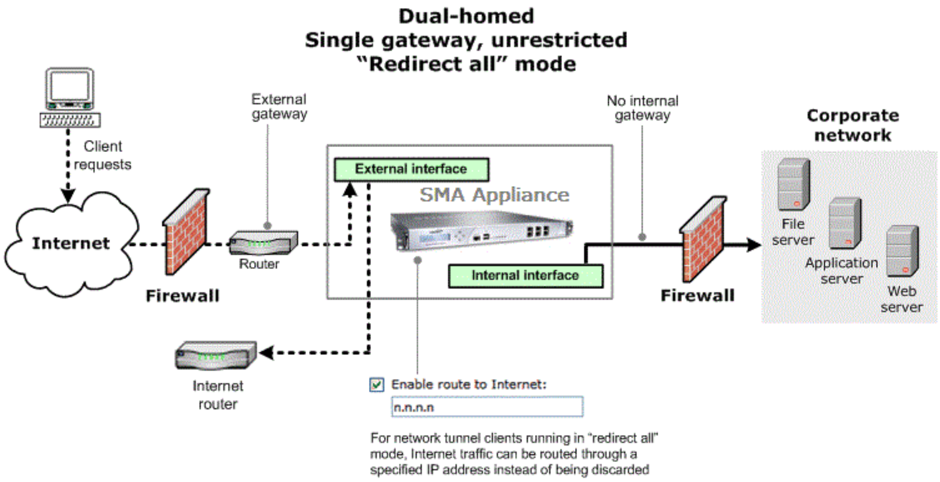
Use the **No gateway** option during evaluation if you will have the interfaces connected to your testing networks without the need for routing.

Scenario 5: Deploying Network Tunnel Clients in "Redirect All" Mode

If you are planning to deploy network tunnel clients in "redirect all" mode, you may need to give your network tunnel users access to both your internal network and the Internet (for more information, see Redirection Modes). This can be accomplished by either of these options:

- Use the **Dual gateway** option, and make certain that your internal gateway router has been configured with a route to the Internet. See the below image.
- Use the **Single gateway**, **unrestricted** option, and then configure the appliance to use a route to the Internet; see Enabling a Route to the Internet.

Deploying Network Tunnel Clients In “Redirect All” Mode



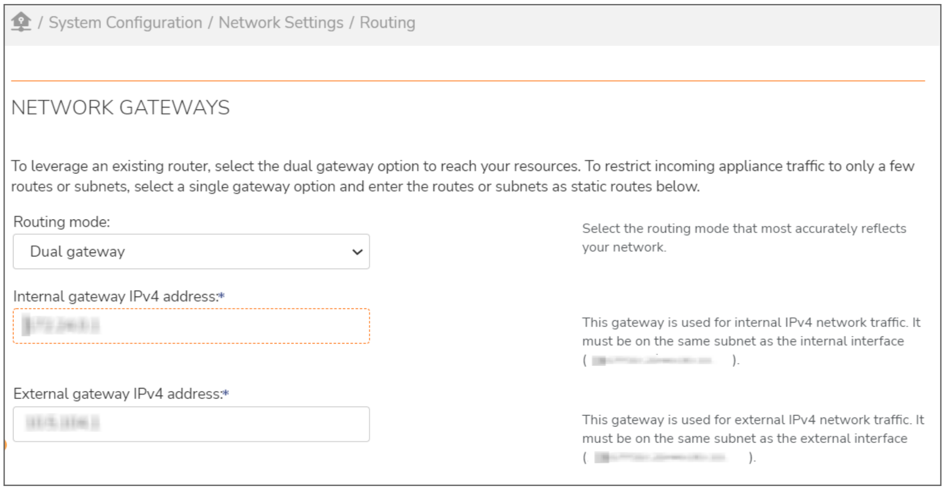
Configuring Network Gateways in a Dual-Homed Environment

The following steps guide you through the setup of network gateways in a dual-homed environment, where both the internal and external interfaces are enabled.

To configure network gateways in a dual-homed environment:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Routing** section, click **Edit**.

   The **Routing** page displays.



/ System Configuration / Network Settings / Routing

NETWORK GATEWAYS

To leverage an existing router, select the dual gateway option to reach your resources. To restrict incoming appliance traffic to only a few routes or subnets, select a single gateway option and enter the routes or subnets as static routes below.

Routing mode:

Dual gateway

Select the routing mode that most accurately reflects your network.

Internal gateway IPv4 address:*

[redacted]

This gateway is used for internal IPv4 network traffic. It must be on the same subnet as the internal interface ([redacted]).

External gateway IPv4 address:*

[redacted]

This gateway is used for external IPv4 network traffic. It must be on the same subnet as the external interface ([redacted]).

3. To route traffic to your network gateways, select a **Routing mode** from these options:

Routing mode	Description
Dual gateway	Specify an IP address for both the external and the internal gateways. Network traffic generated in response to client requests will be sent to the external gateway. All other traffic that does not have a static route defined will be sent to the internal gateway.
Single gateway, restricted	Specify an IP address for just the external gateway. All other traffic that does not have a static route defined will be discarded.
Single gateway, unrestricted	Specify an IP address to be used as both the external and internal gateway. Network traffic not matching a static route will be sent to the external gateway.
No gateway	Network traffic received by the appliance but not matching a static route is discarded.

4. Click **Save**.

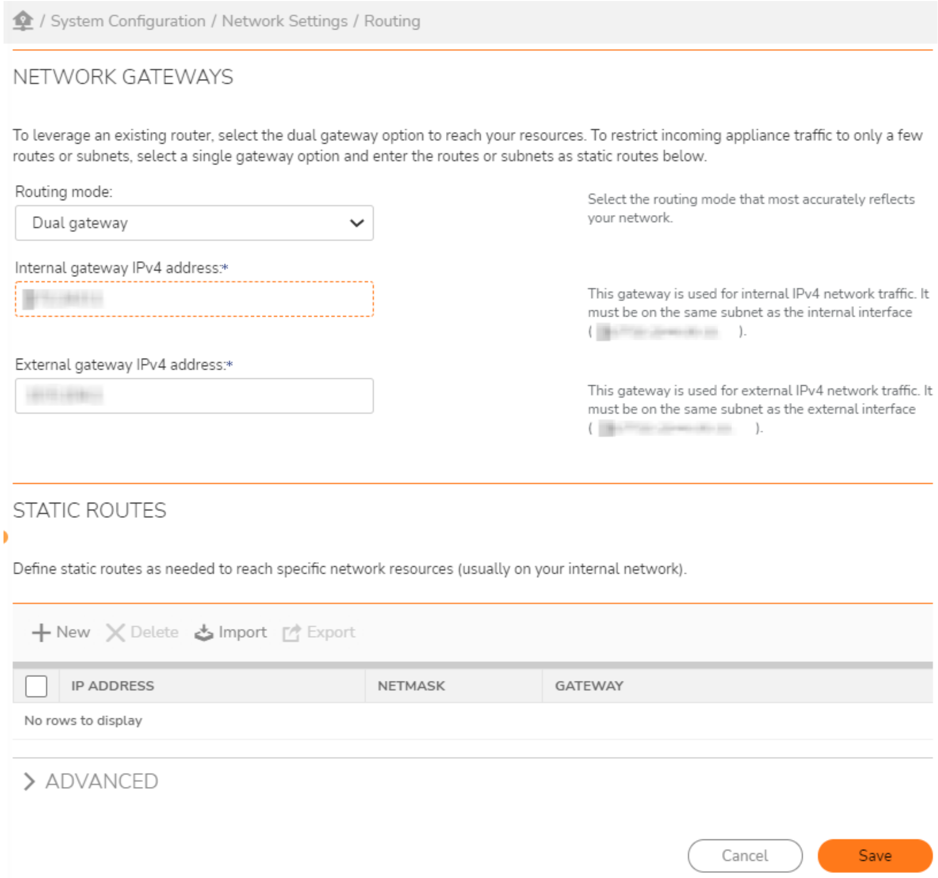
Configuring Network Gateways in a Single-Homed Environment

The following steps guide you through the setup of network gateways in a single-homed environment, where only the internal interface is enabled. This configuration is less common than one that is dual-homed.

To configure a network gateway in a single-homed environment:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Routing** section, click **Edit.**

The **Routing** page displays.



/ System Configuration / Network Settings / Routing

NETWORK GATEWAYS

To leverage an existing router, select the dual gateway option to reach your resources. To restrict incoming appliance traffic to only a few routes or subnets, select a single gateway option and enter the routes or subnets as static routes below.

Routing mode: Dual gateway

Select the routing mode that most accurately reflects your network.

Internal gateway IPv4 address:* [redacted]

This gateway is used for internal IPv4 network traffic. It must be on the same subnet as the internal interface ([redacted]).

External gateway IPv4 address:* [redacted]

This gateway is used for external IPv4 network traffic. It must be on the same subnet as the external interface ([redacted]).

STATIC ROUTES

Define static routes as needed to reach specific network resources (usually on your internal network).

□ IP ADDRESS	NETMASK	GATEWAY
No rows to display		

3. To route traffic to your network gateway, select one of these routing modes:

   - **Default gateway**—Specify an IP address for the default gateway. Network traffic received by the appliance, but not matching a static route will be sent to this address.
   - **No gateway**—Network traffic received by the appliance, but not matching a static route is discarded.

4. Click **Save**.

Enabling a Route to the Internet

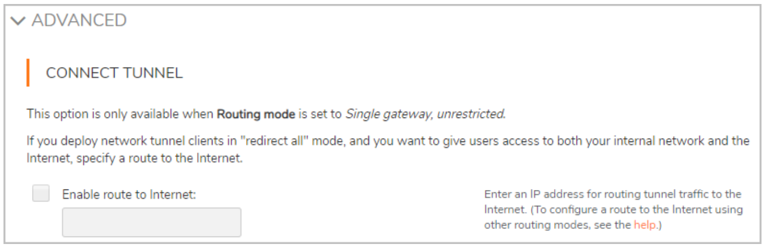
If **Routing mode** is set to **Single gateway**, **unrestricted** you can still enable a route to the Internet for your network tunnel clients, provided your appliance is dual-homed (both internal and external interfaces are enabled). When **Enable route to Internet** is set, all tunnel traffic originating from the client and destined for the Internet (running in “redirect all” mode) will be routed to the specified IP address instead of being discarded.

To enable a route to the Internet:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Routing** section, click **Edit**.

   The **Routing** page displays.
3. Expand the **Advanced** section.

   The **Connect Tunnel** area appears.



ADVANCED

CONNECT TUNNEL

This option is only available when **Routing mode** is set to *Single gateway, unrestricted.*

If you deploy network tunnel clients in "redirect all" mode, and you want to give users access to both your internal network and the Internet, specify a route to the Internet.

□ Enable route to Internet:

Enter an IP address for routing tunnel traffic to the Internet. (To configure a route to the Internet using other routing modes, see the help.)

4. Select the **Enable route to Internet** checkbox, and then type the IP address of your Internet router.
5. Click **Save**.

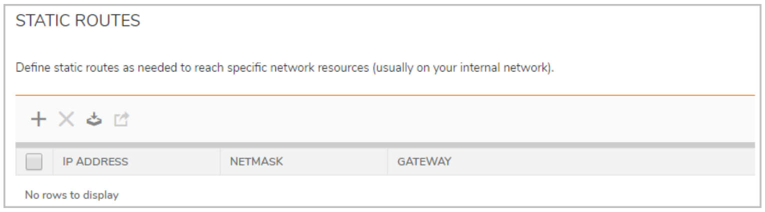
Configuring Static Routes

Static routes are added as entries to the routing table for networks reached from the internal interface. Managing static route tables can be cumbersome, especially at a large site: you may want to create and edit the routing information in a comma-separated value (CSV) text file outside of AMC and then import it. Static route information that you import into AMC must be in an ASCII text file, with each entry on a new line (separated from the previous entry by a CR/LF), and three values separated by commas: IP address, netmask, and gateway. When you import a file, its contents entirely replace any static routes currently specified in AMC.

To configure static routing information:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Routing** section, click **Edit**.

   The **Routing** page displays.
3. In the **Static Routes** section, you can add or modify list entries one by one or as a group:



STATIC ROUTES

Define static routes as needed to reach specific network resources (usually on your internal network).

□	IP ADDRESS	NETMASK	GATEWAY

No rows to display

   - Add a single entry by clicking the **+** (New) icon, and then typing the route information in the **IP address**, **Netmask**, and **Gateway** fields. To modify a list entry, click its link, and then make your changes. After you add or modify an entry, click **OK**.

    - Click **Import** to select the static route table you want to import. The static route information must be in an ASCII text file in CSV format. Each entry must be on a new line (separated from the previous entry by a CR/LF), and must have three values separated by commas: IP address, netmask, and gateway. When you import a file, its contents entirely replace any static routes currently specified in AMC.
    - To modify an existing list of routes, you must either click the list item that you want to change, or export the entire list, modify its contents, and then import it.
4. Click **Save** when you are finished making changes.

To delete a static route:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. On the **Routing** page, select the checkbox to the left of any static routes you want to remove, and then click **Delete**.
3. Click **Save**.

Configuring Name Resolution

The appliance needs access to DNS servers to resolve host names to IP addresses. If you use WorkPlace to browse Windows networks, you also need to specify a WINS (Windows Internet Name Service) server and Windows domain name.

Topics:

- Configuring Domain Name Service
- Configuring Windows Network Name Resolution

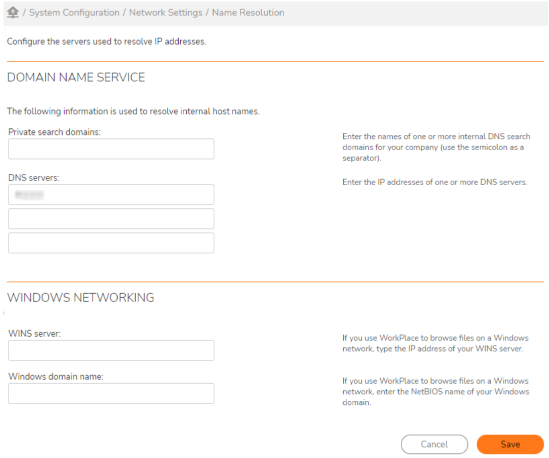
Configuring Domain Name Service

Configuring a DNS server enables the appliance to resolve host names. Properly configuring DNS ensures that the appliance can provide access to your network resources.

To configure DNS name resolution:

1. In the AMC, navigate to **System Configuration > Network Settings**.
    a. In the Name **Resolution** section, click **Edit**.

       The Name **Resolution** page displays.



/ System Configuration / Network Settings / Name Resolution

Configure the servers used to resolve IP addresses.

DOMAIN NAME SERVICE

The following information is used to resolve internal host names.

Private search domains:

Enter the names of one or more internal DNS search domains for your company (use the semicolon as a separator).

DNS servers: [redacted]

Enter the IP addresses of one or more DNS servers.

WINDOWS NETWORKING

WINS server:

If you use WorkPlace to browse files on a Windows network, type the IP address of your WINS server.

Windows domain name:

If you use WorkPlace to browse files on a Windows network, enter the NetBIOS name of your Windows domain.

2. In the **Private search domains** field, type one or more DNS domain names for your company with a semicolon (;) separator (such as `example.com; sales.example.com`). This domain name will be appended to unqualified host names to resolve them. You can enter a maximum of six domain names, separated by semicolons.
3. In the **DNS servers** fields, type the IP addresses of your primary and (if applicable) backup DNS servers. The backup servers are used if the primary server is unavailable.

   > ⓘ **NOTE:** Although three DNS fields are provided, only the first two DNS values will be used for Windows-based clients.

4. Click **Save**.

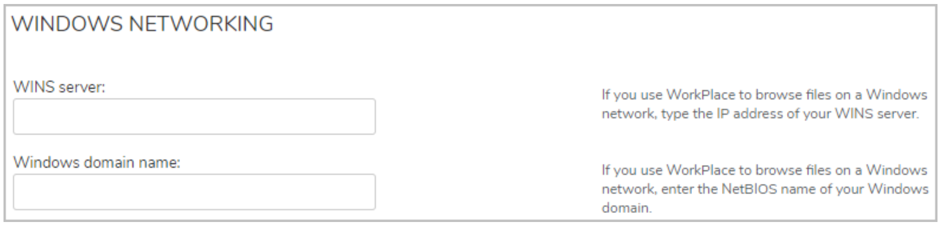
Configuring Windows Network Name Resolution

If you want to browse files on a Windows network using WorkPlace, you must specify a WINS (Windows Internet Name Service) server and a Windows domain name. WorkPlace uses this information to perform name resolution and build a list of resources for users to browse.

To configure Windows network name resolution:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the Name **Resolution** area, click **Edit**.

   The Name **Resolution** page displays.
3. In the **Windows Networking** area, enter:



WINDOWS NETWORKING

WINS server:

If you use WorkPlace to browse files on a Windows network, type the IP address of your WINS server.

Windows domain name:

If you use WorkPlace to browse files on a Windows network, enter the NetBIOS name of your Windows domain.

- The IP address of your primary and (if applicable) secondary WINS server.
- Your **Windows domain name** using NetBIOS syntax (for example, `mycompany`).

  ⓘ **IMPORTANT:** If you are not using a WINS server, do not enter a value in the **Windows domain name** field.

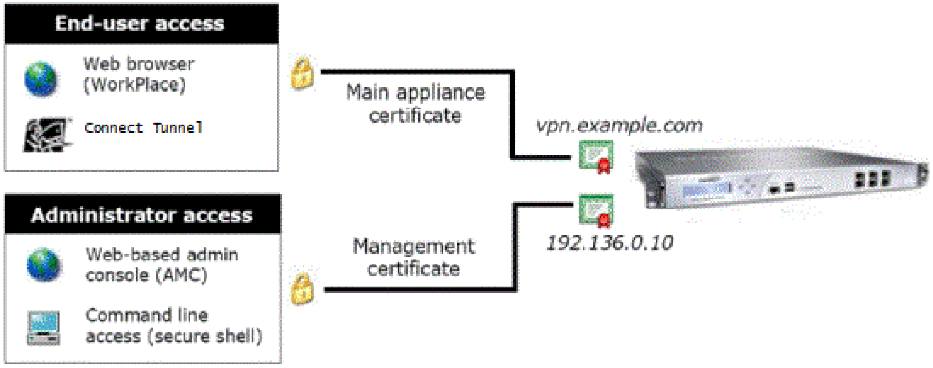
4. Click **Save**.

Certificates

The SMA appliance uses SSL certificates to secure information that the client computer sends to the server, and to validate the appliance's identity to connecting users; see the below image:

- The Secure Mobile Access services use a certificate to secure user traffic from a Web browser to WorkPlace, and from the Connect clients to the appliance. (If you want to provide several WorkPlace sites, you can use a wildcard certificate for multiple sites, or associate a different certificate with each one. In either case, the sites can have different host and domain names; for more information, see Adding WorkPlace Sites.)
- AMC uses a separate certificate to secure management traffic.

  Certificate Usage



Subject Alternative Name (SAN) certificates are supported for Workplace, Workplace sites, and Connect Tunnel. These certificates are used to securely encrypt communication channels between a set of clients and multiple distinct SSL or TLS services.

SAN certificates simplify the IP address/hostname/certificate sets needed for a typical deployment. With a single SAN certificate, you can utilize one IP address with multiple distinct SSL or TLS protected web or client/server services, without the need for configuring additional IP addresses. Additionally, SANs can be used for different host names on the same IP address, alleviating the need for a one-to-one mapping of SSL certificate Common Names to FQDN.

The Administrator can generate, import, process, and otherwise use a SAN certificate for Workplace, ActiveSync, Custom FQDN URL Mapping, or Tunnel-based access services.

CA certificates are also used for securing connections to back-end servers and authentication using client certificates. See Importing CA Certificates for more details.

Topics:

- Server Certificates
- CA Certificates
- Working with Certificates FAQs

Let's Encrypt

Let’s Encrypt is a certificate authority that is public, free, API-driven, and trusted by browsers/clients. Integrating a Let's Encrypt certificate with SMA enhances security and eases the deployment process. Let's Encrypt certificates are valid for 90 days and are renewed automatically after 60 days.

Let's Encrypt certificates can be configured for standalone and CMS/GTO deployments where CMS manages the Let’s Encrypt certificate(s) for the cluster.

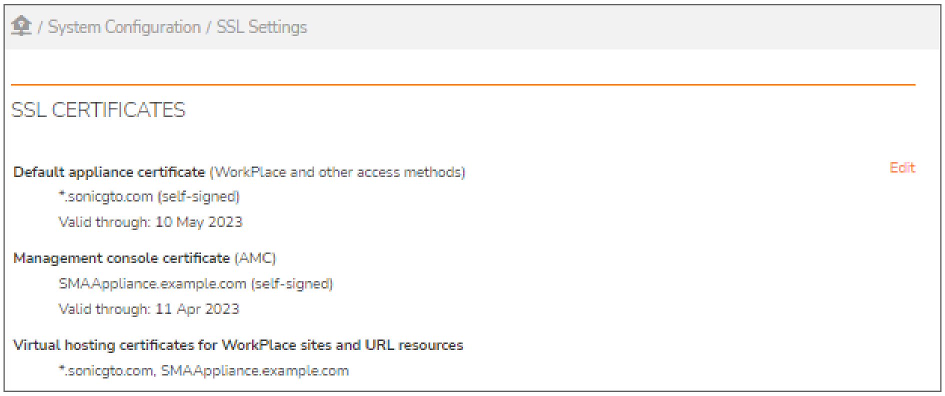
Prerequisites:

- The appliance must be able to access the Let's Encrypt signing CA over the internet.
- Let's Encrypt signing CA must be able to resolve all the Subject Alternative Name (SAN) names included in the certificate in public DNS.
- All the SAN names must resolve to the public IP address of the standalone appliance.
- The Let's Encrypt signing CA must be able to access port 443 on the public interface (or via NAT, as long as the name resolves).

Creating a Let's Encrypt certificate

To create a Let's Encrypt certificate in AMC:

1. Log in to AMC.
2. Navigate to **System Configuration** > **SSL Settings**.
3. Click **Edit** under the **SSL Certificates** group.

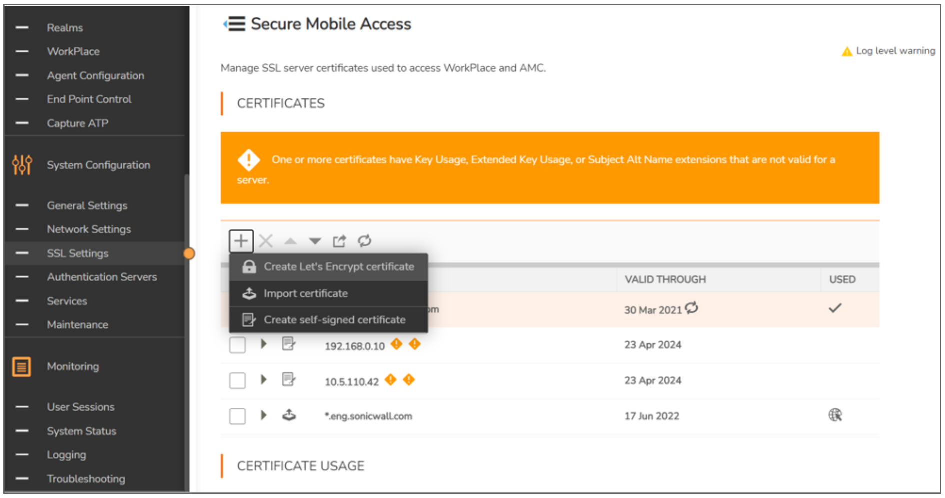


Default appliance certificate (WorkPlace and other access methods)
*.sonicgto.com (self-signed)
Valid through: 10 May 2023

Management console certificate (AMC)
SMAAppliance.example.com (self-signed)
Valid through: 11 Apr 2023

Virtual hosting certificates for WorkPlace sites and URL resources
*.sonicgto.com, SMAAppliance.example.com

4. To create a certificate, click + icon and select **Create Let's Encrypt certificate** option.



Manage SSL server certificates used to access WorkPlace and AMC.

One or more certificates have Key Usage, Extended Key Usage, or Subject Alt Name extensions that are not valid for a server.

	VALID THROUGH	USED
om	30 Mar 2021	✓
192.168.0.10	23 Apr 2024	
10.5.110.42	23 Apr 2024	
*.eng.sonicwall.com	17 Jun 2022	

5. In the **Fully qualified domain name** field, enter the complete domain name. The FQDN entered here appears in the certificate and visible to users. You must also add FQDN to your DNS.

   ⓘ | **NOTE:** Wildcard characters are not supported in the FQDN field.

6. In the **Alternatives names** field, enter any other name for FQDN. The alternative name entered here appears in the certificate using the Subject Alternative Name (SAN) certificate extension.

   ⓘ | **NOTE:** Let's Encrypt supports up to 100 SANs per certificate.

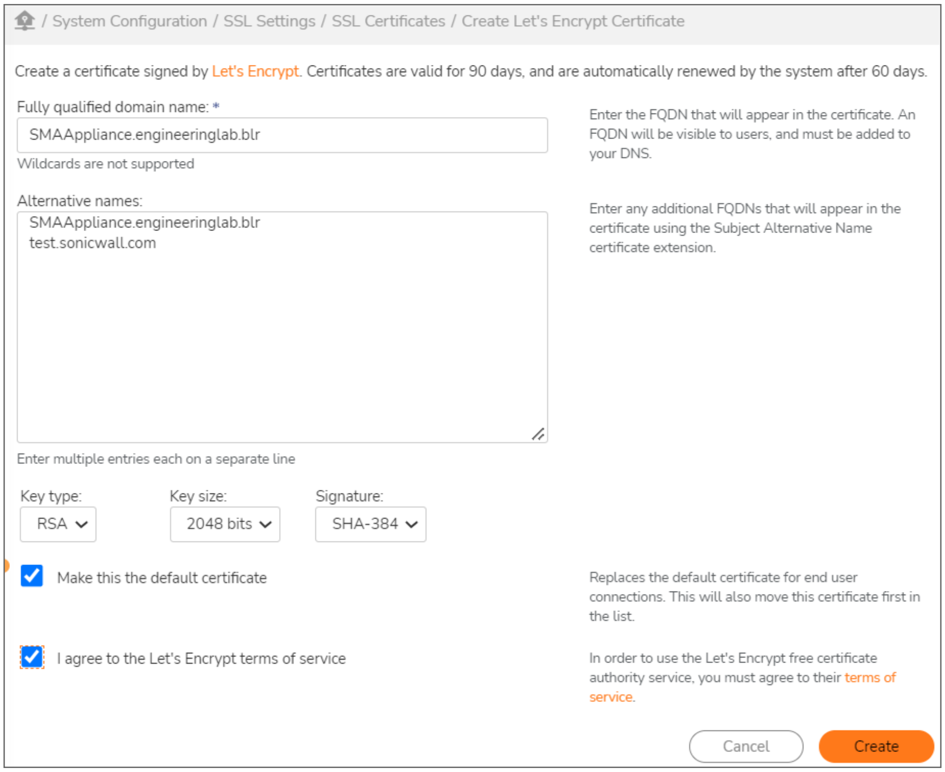
7. In the **Key type** drop-down field, select the key type based on your requirement. The supported key types are RSA and EC.

8. In the **Key size** drop-down field, select the key size based on your requirement. The supported key sizes are 2048, 3072, and 4096 bits.

9. In the **Signature** drop-down field, select the secure hash algorithm based on your requirement. The supported signatures are SHA 512, SHA-384, and SHA-256.

10. Select **Make this the default certificate** check box. Selecting this check box replaces the default certificate for end user connections and moves the certificate to first in the list.

11. In order to use the Let's Encrypt free certificate authority service, you must agree to their terms of service. Select **I agree to the Let's Encrypt terms of service** check box.



/ System Configuration / SSL Settings / SSL Certificates / Create Let's Encrypt Certificate

Create a certificate signed by Let's Encrypt. Certificates are valid for 90 days, and are automatically renewed by the system after 60 days.

Fully qualified domain name: * SMAAppliance.engineeringlab.blr

Wildcards are not supported

Enter the FQDN that will appear in the certificate. An FQDN will be visible to users, and must be added to your DNS.

Alternative names:

SMAAppliance.engineeringlab.blr
test.sonicwall.com

Enter multiple entries each on a separate line

Enter any additional FQDNs that will appear in the certificate using the Subject Alternative Name certificate extension.

Key type: RSA

Key size: 2048 bits

Signature: SHA-384

☑ Make this the default certificate

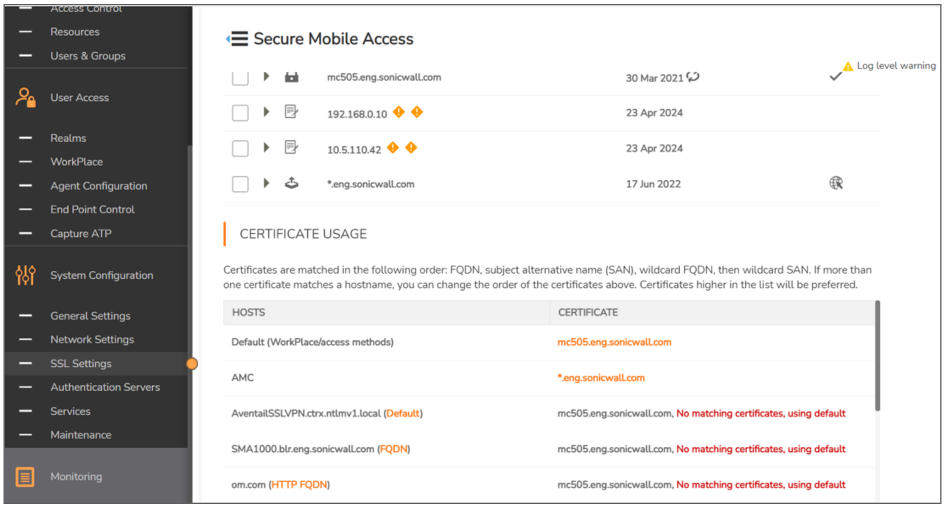
Replaces the default certificate for end user connections. This will also move this certificate first in the list.

☑ I agree to the Let's Encrypt terms of service

In order to use the Let's Encrypt free certificate authority service, you must agree to their terms of service.

12. Click **Create**.

    The Let's Encrypt certificate is created and you can view them under **System Configuration** > **SSL Settings**.



mc505.eng.sonicwall.com	30 Mar 2021
192.168.0.10	23 Apr 2024
10.5.110.42	23 Apr 2024
*.eng.sonicwall.com	17 Jun 2022

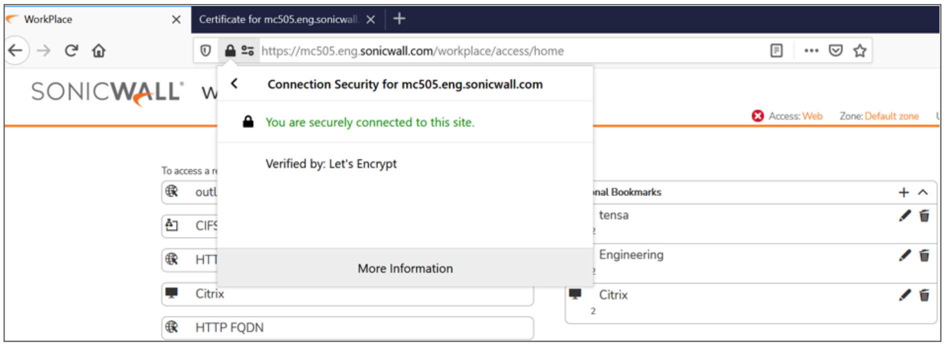
CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	mc505.eng.sonicwall.com
AMC	*.eng.sonicwall.com
AventailSSLVPN.ctrx.ntlmv1.local (Default)	mc505.eng.sonicwall.com, No matching certificates, using default
SMA1000.blr.eng.sonicwall.com (FQDN)	mc505.eng.sonicwall.com, No matching certificates, using default
om.com (HTTP FQDN)	mc505.eng.sonicwall.com, No matching certificates, using default

13. Click **Apply Pending Changes**.

Once you completed creating a Let's Encrpyt certificate, browse to the host name and ensure that the certificate is valid and verified.



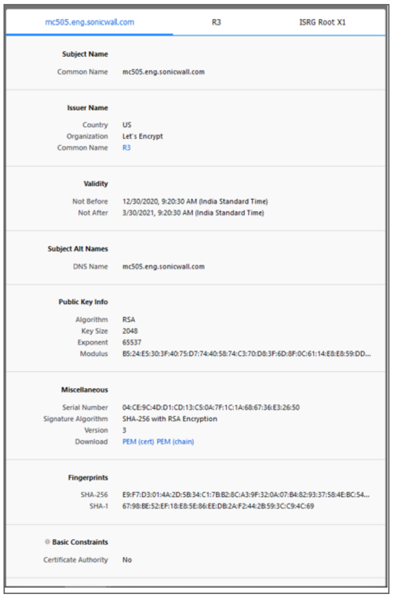
Connection Security for mc505.eng.sonicwall.com

You are securely connected to this site.

Verified by: Let's Encrypt

More Information

Click **More information** to view the validity period and other details.



mc505.eng.sonicwall.com | R3 | ISRG Root X1

Subject Name

Common Name: mc505.eng.sonicwall.com

Issuer Name

Country: US
Organization: Let's Encrypt
Common Name: R3

Validity

Not Before: 12/30/2020, 9:20:30 AM (India Standard Time)
Not After: 3/30/2021, 9:20:30 AM (India Standard Time)

Subject Alt Names

DNS Name: mc505.eng.sonicwall.com

Public Key Info

Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus: B5:24:E5:30:3F:40:75:D7:74:40:58:74:C3:70:D8:3F:6D:8F:0C:61:14:E8:E8:59:DD...

Miscellaneous

Serial Number: 04:CE:9C:4D:D1:CD:13:C5:0A:7F:1C:1A:68:67:36:E3:26:50
Signature Algorithm: SHA-256 with RSA Encryption
Version: 3
Download: PEM (cert) PEM (chain)

Fingerprints

SHA-256: E9:F7:D3:01:4A:2D:5B:34:C1:7B:B2:8C:A3:9F:32:0A:07:B4:82:93:37:58:4E:BC:54...
SHA-1: 67:98:BE:52:EF:18:E8:5E:86:EE:DB:2A:F2:44:2B:59:3C:C9:4C:69

Basic Constraints

Certificate Authority: No

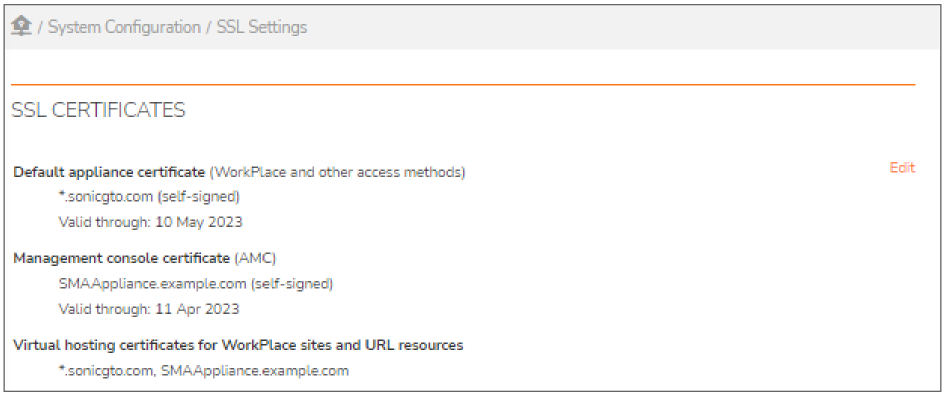
Renewing the certificate

Let's Encrypt certificates are valid for 90 days and are renewed automatically after 60 days. You can also renew it manually based on your requirements.

ⓘ **NOTE:** If your list of FQDNs changes, then you need to create a new Let's Encrypt certificate rather than renewing the certificate.

To renew the certificate manually:

1. Log in to AMC.
2. Navigate to **System Configuration** > **SSL Settings**.
3. Click **Edit** under the **SSL Certificates** group.



SSL CERTIFICATES

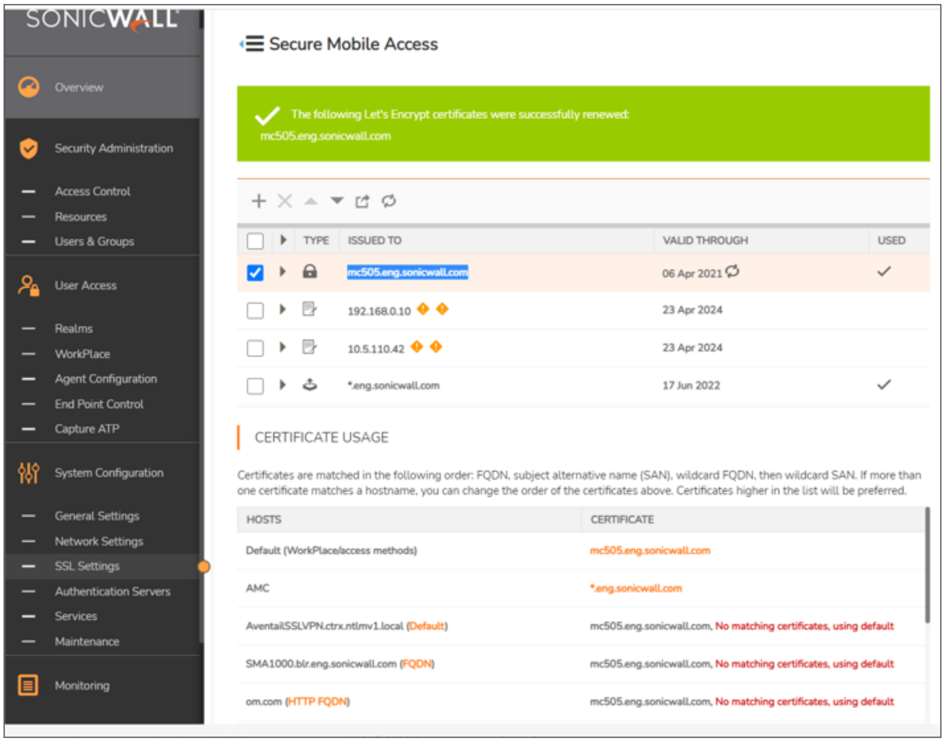
Default appliance certificate (WorkPlace and other access methods)
*.sonicgto.com (self-signed)
Valid through: 10 May 2023

Management console certificate (AMC)
SMAAppliance.example.com (self-signed)
Valid through: 11 Apr 2023

Virtual hosting certificates for WorkPlace sites and URL resources
*.sonicgto.com, SMAAppliance.example.com

4. In the **General** tab, select the certificate you want to renew and click ⟳.

   A success message is displayed and the certificate is renewed for the next 90 days. You can view the certificate validity updated under **Valid Through** field.



The following Let's Encrypt certificates were successfully renewed:
mc505.eng.sonicwall.com

□		TYPE	ISSUED TO	VALID THROUGH	USED
☑	▸	🔒	mc505.eng.sonicwall.com	06 Apr 2021 ⟳	✓
□	▸		192.168.0.10	23 Apr 2024	
□	▸		10.5.110.42	23 Apr 2024	
□	▸		*.eng.sonicwall.com	17 Jun 2022	✓

CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

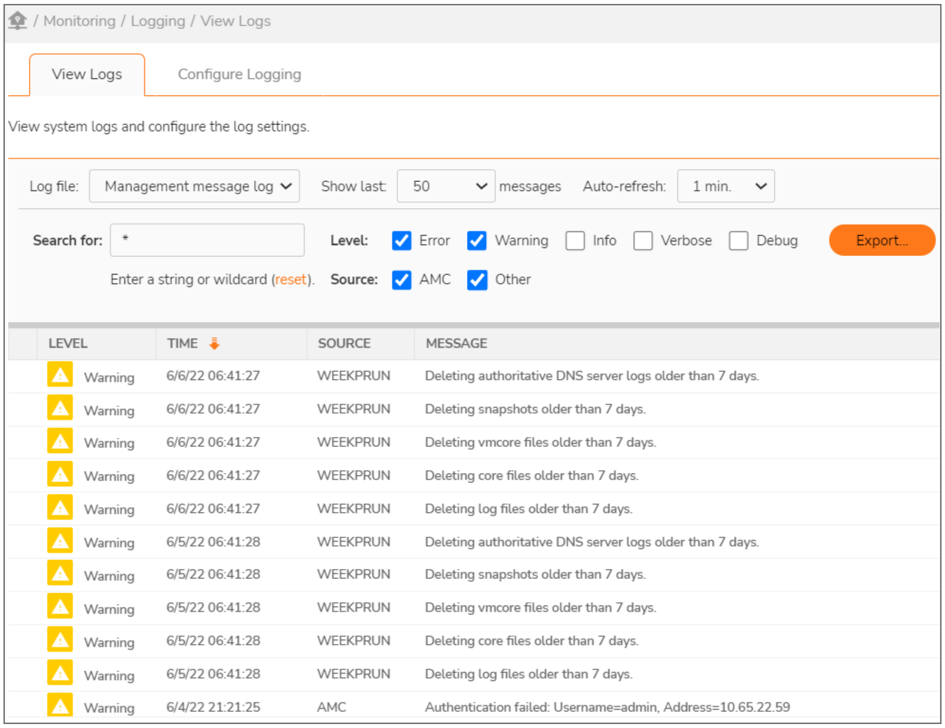
HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	mc505.eng.sonicwall.com
AMC	*.eng.sonicwall.com
AventailSSLVPN.ctrx.ntlmv1.local (Default)	mc505.eng.sonicwall.com, No matching certificates, using default
SMA1000.blr.eng.sonicwall.com (FQDN)	mc505.eng.sonicwall.com, No matching certificates, using default
om.com (HTTP FQDN)	mc505.eng.sonicwall.com, No matching certificates, using default

Viewing the Logs

The SMA appliance records system and user events in a series of log files. The creation of a Let's Encrypt certificate and the changes made on the certificate are captured in the Logs.

To view the logs:

1. Log in to AMC.
2. Navigate to **Monitoring** > **Logging**.
   All the events on Let's Encrypt certificate are displayed under the Management audit log file.



View system logs and configure the log settings.

Log file: Management message log | Show last: 50 messages | Auto-refresh: 1 min.

Search for: * | Level: ☑ Error ☑ Warning □ Info □ Verbose □ Debug | Export...

Enter a string or wildcard (reset). | Source: ☑ AMC ☑ Other

LEVEL	TIME	SOURCE	MESSAGE
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting core files older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting log files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting core files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting log files older than 7 days.
Warning	6/4/22 21:21:25	AMC	Authentication failed: Username=admin, Address=10.65.22.59

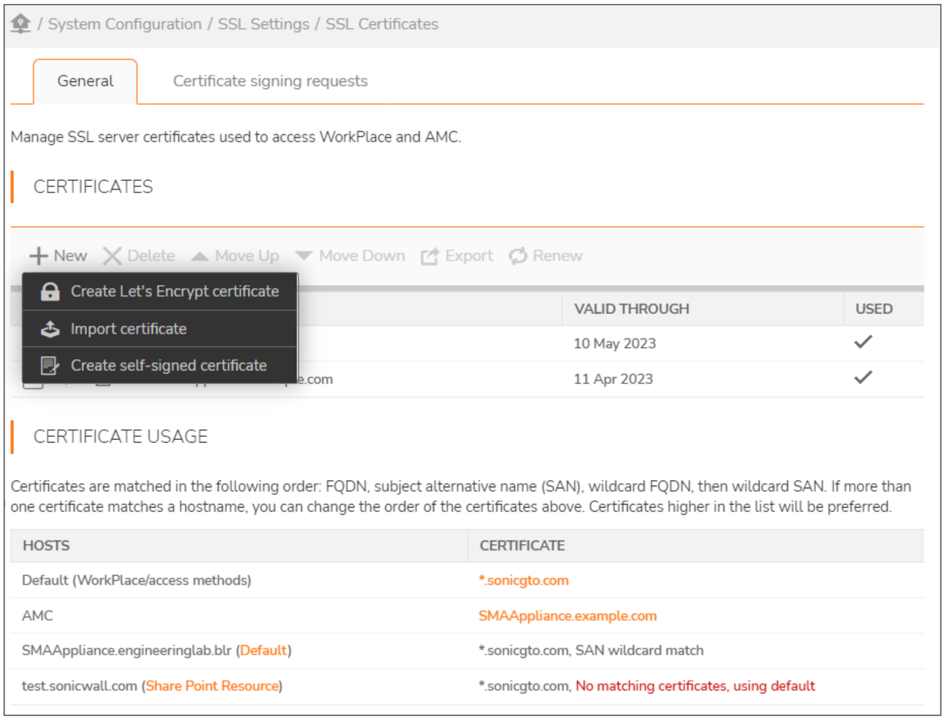
Creating a Let's Encrypt certificate in CMS

Prerequisites:

- The CMS must be able to access the Let's Encrypt signing CA over the internet.
- All GTO service names must be delegated in public DNS so that queries are resolved by the GTO authoritative servers.
- The Let's Encrypt signing CA MUST be able to access port 443 on all managed appliances public interface(s) (via NAT and is connected using name).
- All the managed appliances should be able to access port 443 in CMS.

To create a Let's Encrypt certificate in CMS:

1. Log in to CMS.
2. Navigate to **Management Server** > **Configure**.
3. Click **Edit** under the **SSL Certificates** group.
4. In the **General** tab, click + icon and select **Create Let's Encrypt certificate**option.


/ System Configuration / SSL Settings / SSL Certificates

General
Certificate signing requests

Manage SSL server certificates used to access WorkPlace and AMC.

CERTIFICATES

New
Delete
Move Up
Move Down
Export
Renew
Create Let's Encrypt certificate
Import certificate
Create self-signed certificate

	VALID THROUGH	USED
	10 May 2023	✓
e.com	11 Apr 2023	✓

CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	*.sonicgto.com
AMC	SMAAppliance.example.com
SMAAppliance.engineeringlab.blr (Default)	*.sonicgto.com, SAN wildcard match
test.sonicwall.com (Share Point Resource)	*.sonicgto.com, No matching certificates, using default

5. In the **Fully qualified domain name** field, enter the complete domain name. The FQDN entered here appears in the certificate and visible to users. You must also add FQDN to your DNS.

   ⓘ | **NOTE:** Wildcard characters are not supported in the FQDN field.

6. In the **Alternatives names** field, enter any other name for FQDN. The alternative name entered here appears in the certificate using the Subject Alternative Name (SAN) certificate extension.

   ⓘ | **NOTE:** Let's Encrypt supports up to 100 SANs per certificate.

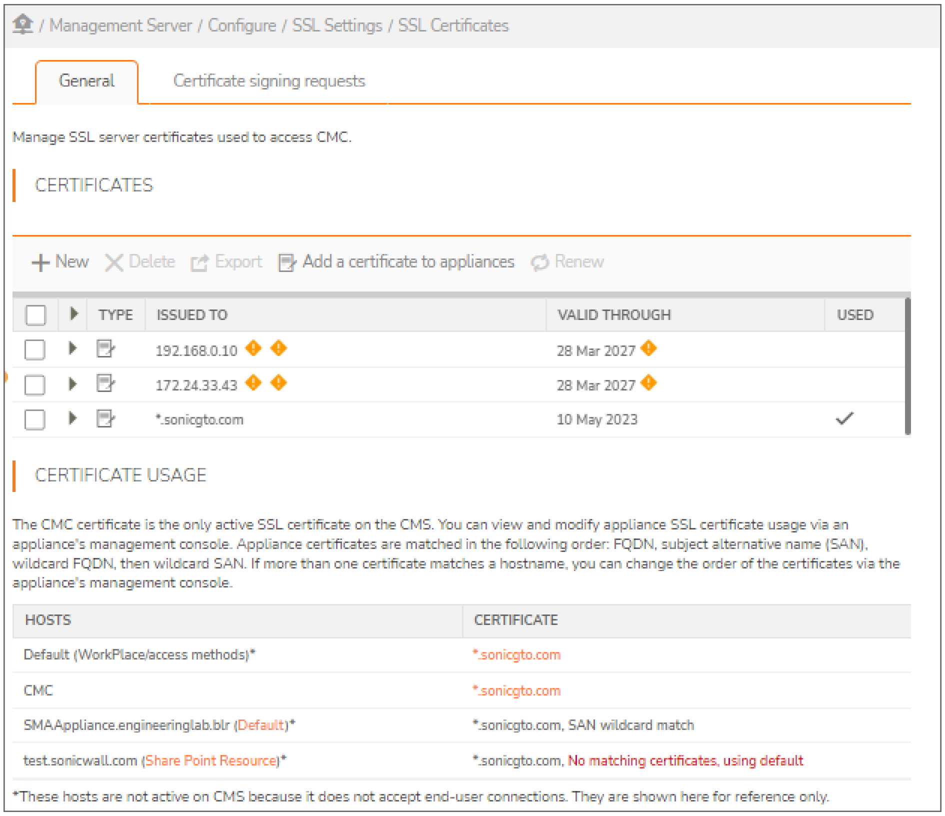
7. In the **Key type** drop-down field, select the key type based on your requirement. The supported key types are RSA and EC.

8. In the **Key size** drop-down field, select the key size based on your requirement. The supported key sizes are 2048, 3072, and 4096 bits.

9. In the **Signature** drop-down field, select the secure hash algorithm based on your requirement. The supported signatures are SHA 512, SHA-384, and SHA-256.

10. Select **Make this the default certificate** check box. Selecting this check box replaces the default certificate for end user connections and moves the certificate to first in the list.

11. In order to use the Let's Encrypt free certificate authority service, you must agree to their terms of service. Select **I agree to the Let's Encrypt terms of service** check box.


/ Management Server / Configure / SSL Settings / SSL Certificates
General
Certificate signing requests
New
Delete
Export
Add a certificate to appliances
Renew

Manage SSL server certificates used to access CMC.

CERTIFICATES

□		TYPE	ISSUED TO	VALID THROUGH	USED
□	▸		192.168.0.10 ◆ ◆	28 Mar 2027 ◆	
□	▸		172.24.33.43 ◆ ◆	28 Mar 2027 ◆	
□	▸		*.sonicgto.com	10 May 2023	✓

CERTIFICATE USAGE

The CMC certificate is the only active SSL certificate on the CMS. You can view and modify appliance SSL certificate usage via an appliance's management console. Appliance certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates via the appliance's management console.

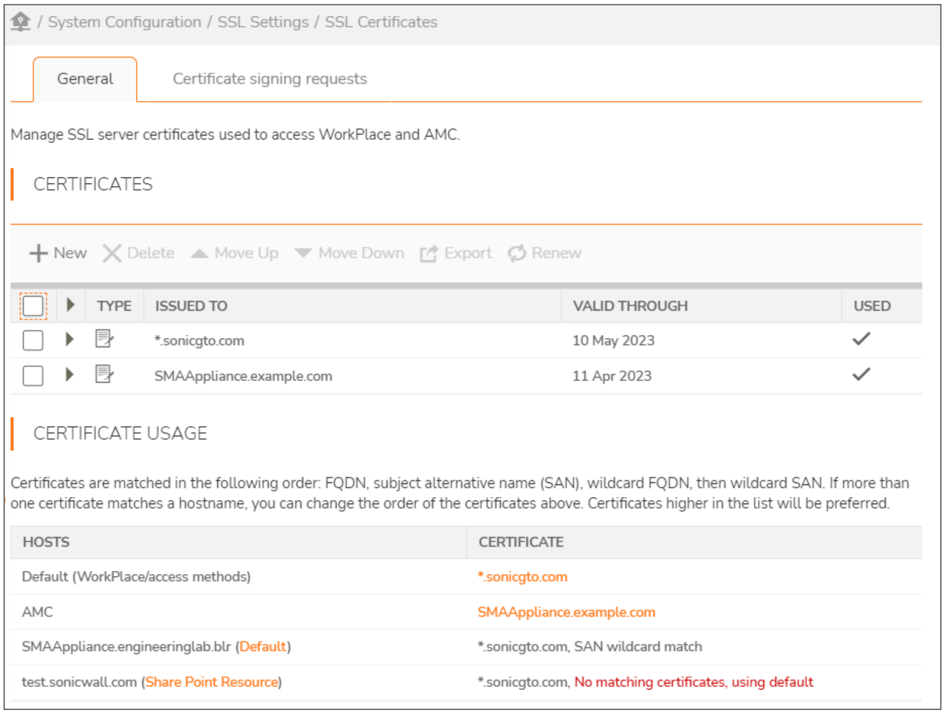
HOSTS	CERTIFICATE
Default (WorkPlace/access methods)*	*.sonicgto.com
CMC	*.sonicgto.com
SMAAppliance.engineeringlab.blr (Default)*	*.sonicgto.com, SAN wildcard match
test.sonicwall.com (Share Point Resource)*	*.sonicgto.com, No matching certificates, using default

*These hosts are not active on CMS because it does not accept end-user connections. They are shown here for reference only.

The Let's Encrypt certificate is created. You can view the Let's Encrypt certificate in AMC.

To view the certificate:

1. Log in to AMC.
2. Navigate to **System Configuration** > **SSL Settings**.



/ System Configuration / SSL Settings / SSL Certificates

Manage SSL server certificates used to access WorkPlace and AMC.

CERTIFICATES

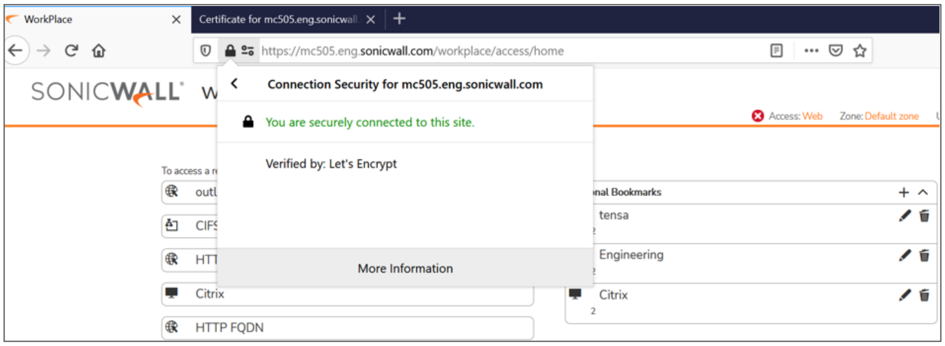
□		TYPE	ISSUED TO	VALID THROUGH	USED
□	▸		*.sonicgto.com	10 May 2023	✓
□	▸		SMAAppliance.example.com	11 Apr 2023	✓

CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	*.sonicgto.com
AMC	SMAAppliance.example.com
SMAAppliance.engineeringlab.blr (Default)	*.sonicgto.com, SAN wildcard match
test.sonicwall.com (Share Point Resource)	*.sonicgto.com, No matching certificates, using default

Once you completed creating a Let's Encrpyt certificate, browse to the host name and ensure that the certificate is valid and verified.



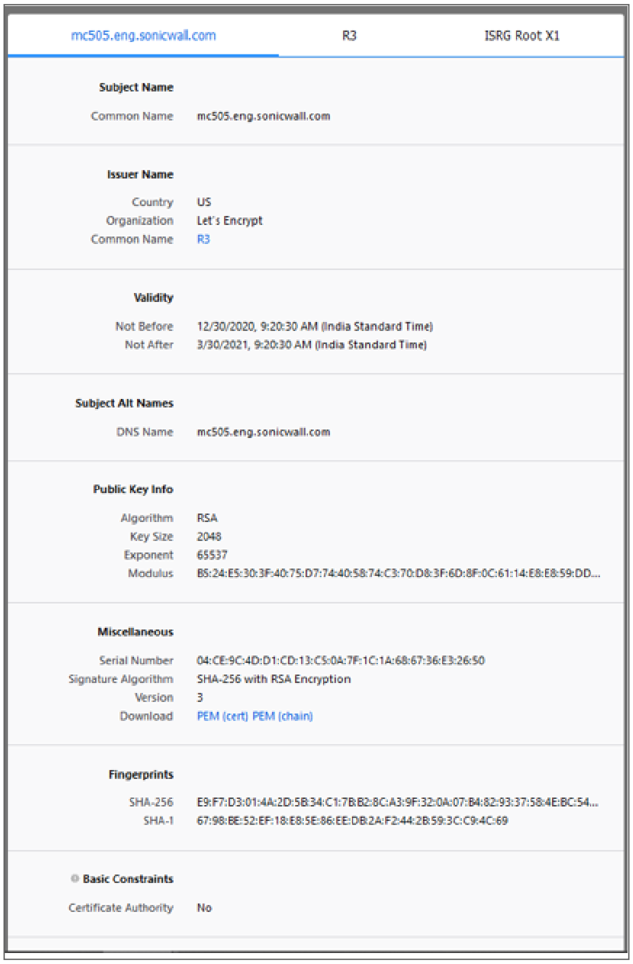
https://mc505.eng.sonicwall.com/workplace/access/home

Connection Security for mc505.eng.sonicwall.com

You are securely connected to this site.

Verified by: Let's Encrypt

Click **More information** to view the validity period and other details.



Subject Name

Common Name	mc505.eng.sonicwall.com

Issuer Name

Country	US
Organization	Let's Encrypt
Common Name	R3

Validity

Not Before	12/30/2020, 9:20:30 AM (India Standard Time)
Not After	3/30/2021, 9:20:30 AM (India Standard Time)

Subject Alt Names

DNS Name	mc505.eng.sonicwall.com

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	B5:24:E5:30:3F:40:75:D7:74:40:58:74:C3:70:D8:3F:6D:8F:0C:61:14:E8:E8:59:DD...

Miscellaneous

Serial Number	04:CE:9C:4D:D1:CD:13:C5:0A:7F:1C:1A:68:67:36:E3:26:50
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	E9:F7:D3:01:4A:2D:5B:34:C1:7B:B2:8C:A3:9F:32:0A:07:B4:82:93:37:58:4E:BC:54...
SHA-1	67:98:BE:52:EF:18:E8:5E:86:EE:DB:2A:F2:44:2B:59:3C:C9:4C:69

Basic Constraints

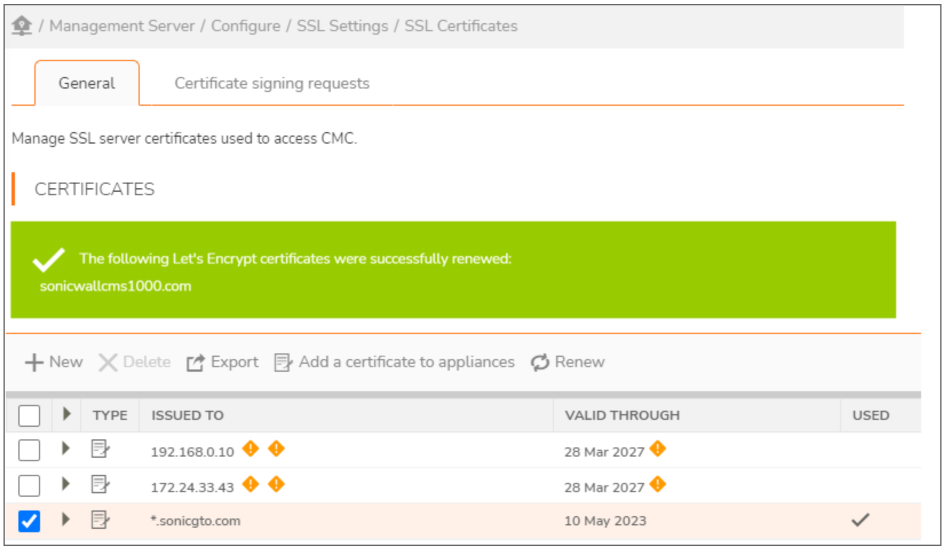
Certificate Authority	No

Renewing the certificate in CMS

The Let's Encrypt certificates are valid for 90 days and is renewed automatically after 60 days. You can also renew it manually based on your requirements.

To renew the certificate manually:

1. Log in to CMS.*:*
2. In the left panel, select **Management Server** > **Configure**.
3. Click **Edit** under the **SSL Certificates** group.
4. In the **General** tab, select the certificate you want to renew and click ⟳.
5. A success message is displayed and the certificate is renewed for the next 90 days. You can view the certificate validity displayed under **Valid Through** field.


/ Management Server / Configure / SSL Settings / SSL Certificates
General
Certificate signing requests

Manage SSL server certificates used to access CMC.

CERTIFICATES

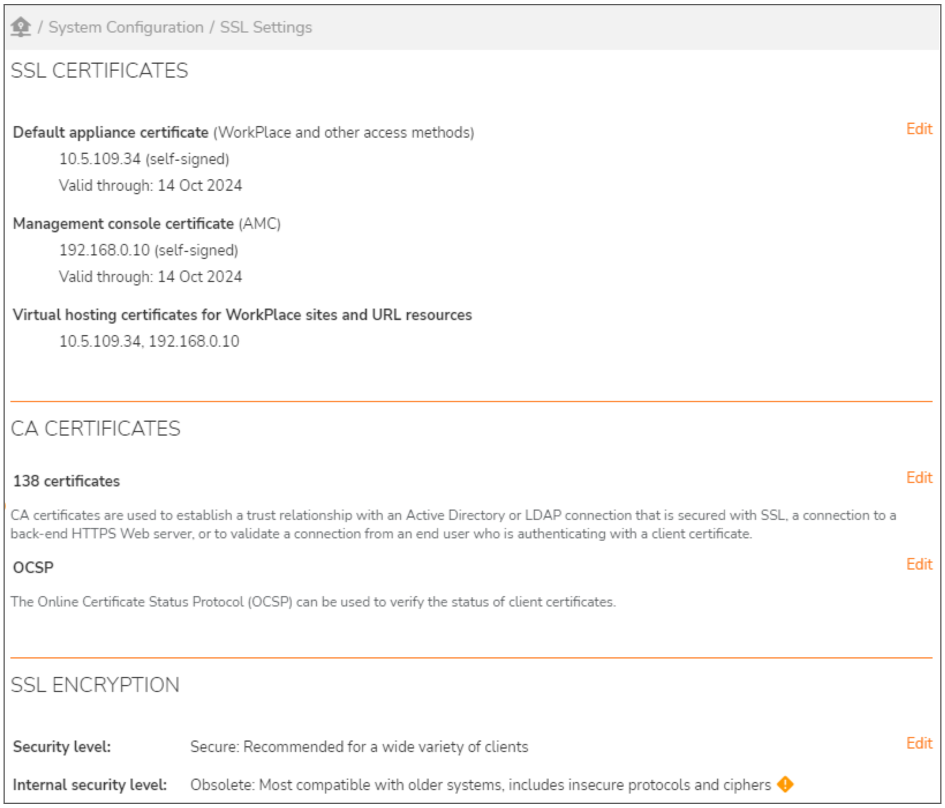
✓ The following Let's Encrypt certificates were successfully renewed:
sonicwallcms1000.com

+ New
Delete
Export
Add a certificate to appliances
Renew

□		TYPE	ISSUED TO	VALID THROUGH	USED
□	▸		192.168.0.10	28 Mar 2027	
□	▸		172.24.33.43	28 Mar 2027	
☑	▸		*.sonicgto.com	10 May 2023	✓

Server Certificates

To manage the SSL server certificates used to access WorkPlace and AMC, navigate to **System Configuration > SSL Settings** in the main navigation menu in AMC.



/ System Configuration / SSL Settings

SSL CERTIFICATES

Default appliance certificate (WorkPlace and other access methods) Edit

10.5.109.34 (self-signed)

Valid through: 14 Oct 2024

Management console certificate (AMC)

192.168.0.10 (self-signed)

Valid through: 14 Oct 2024

Virtual hosting certificates for WorkPlace sites and URL resources

10.5.109.34, 192.168.0.10

CA CERTIFICATES

138 certificates Edit

CA certificates are used to establish a trust relationship with an Active Directory or LDAP connection that is secured with SSL, a connection to a back-end HTTPS Web server, or to validate a connection from an end user who is authenticating with a client certificate.

OCSP Edit

The Online Certificate Status Protocol (OCSP) can be used to verify the status of client certificates.

SSL ENCRYPTION

Security level: Secure: Recommended for a wide variety of clients Edit

Internal security level: Obsolete: Most compatible with older systems, includes insecure protocols and ciphers

This is where you view, import, and delete SSL and CA certificates.

- Certificate Strategy
- Obtaining a Certificate from a Commercial CA
- Creating a Self-Signed Certificate
- Managing Server Certificates in AMC

Certificate Strategy

There are three types of certificates:

- Let’s Encrypt, is a certificate authority that is public, free, API-driven, and trusted by browsers/clients.
- A **commercial CA** verifies your company’s identity, vouching for your identity by providing you with a certificate that the CA signs. A CA need not be commercial or third-party—a company can be its own CA. Commercial certificates are purchased from a CA such as Symantec (http://www.symantec.com/ssl-certificates), and are usually valid for one year.
- With a **self-signed SSL certificate**, you are verifying your own identity. The associated private key data is encrypted using a password. A self-signed certificate can also be a wildcard certificate, allowing it to be used by multiple servers which share the same IP address and certificate, but have different FQDNs.

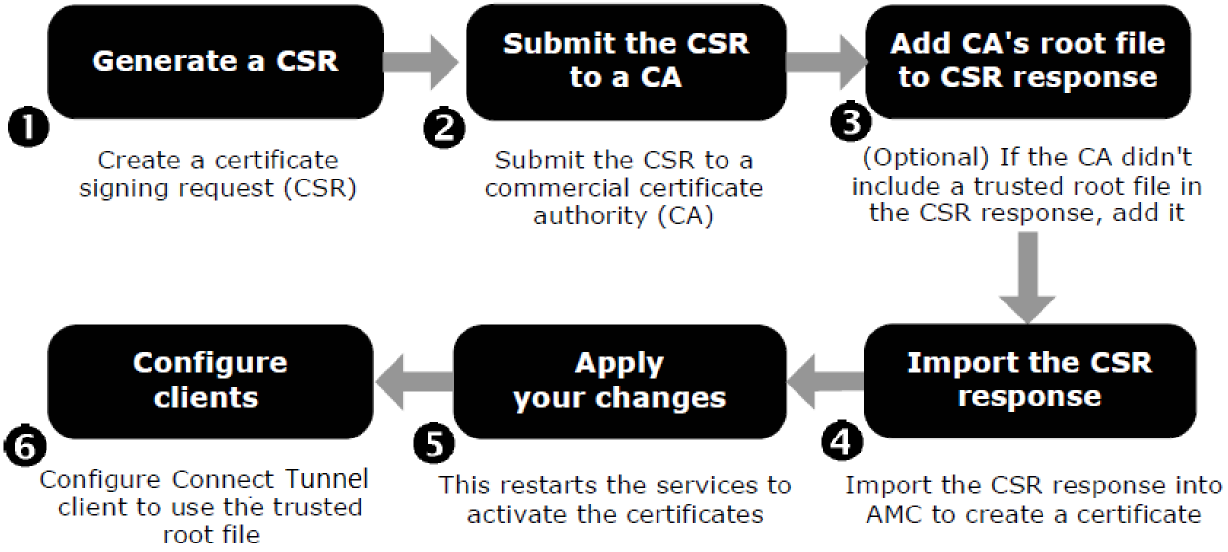
When deciding which type of certificate to use for the servers, consider who will be connecting to the appliance and how they will use resources on your network. If business partners are connecting to Web resources through the appliance, they will likely want some assurance of your identity before performing a transaction or providing confidential information. In this case, you would probably want to obtain a certificate from a commercial CA for the appliance.

△ **CAUTION: When the appliance is configured with a certificate from a CA that is not well known or one that is self-signed, small form factor device users may see an error message and be unable to log in. For more information on small form factor devices, see WorkPlace and Small Form Factor Devices.**

Obtaining a Certificate from a Commercial CA

Obtaining a certificate from a commercial CA provides verification of your identity for people who connect to your network through the appliance. You must perform several steps to obtain and configure a certificate from a commercial CA, as shown in the below image.

Obtaining CA Certificate



Create a certificate signing request (CSR)

Submit the CSR to a commercial certificate authority (CA)

(Optional) If the CA didn't include a trusted root file in the CSR response, add it

Import the CSR response into AMC to create a certificate

This restarts the services to activate the certificates

Configure Connect Tunnel client to use the trusted root file

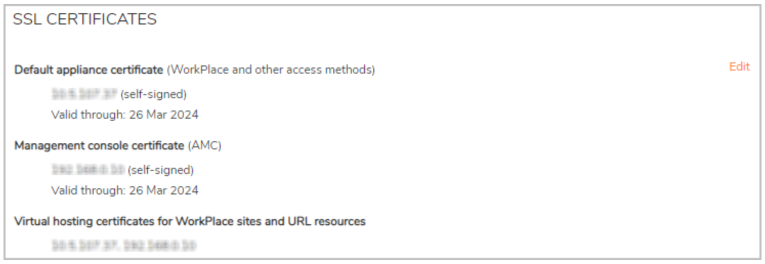
- Step 1: Generate a Certificate Signing Request
- Step 2: Submit the CSR to a Commercial CA
- Step 3: Review CSR Response and Add CA's Root Certificate
- Step 4: Import the CSR Response Into AMC
- Step 5: Apply Your Changes

Step 1: Generate a Certificate Signing Request

Using AMC, you can generate a certificate signing request (CSR). This process creates an RSA key pair that is used to secure server information, and a CSR containing your public key and identity information. The information you provide is used by the commercial CA to generate your certificate, and may be visible to users who connect to the appliance.

To generate a CSR:

1. In the AMC, navigate to **System Configuration > SSL Settings**.



SSL CERTIFICATES

Default appliance certificate (WorkPlace and other access methods)

[redacted] (self-signed)
Valid through: 26 Mar 2024

Management console certificate (AMC)

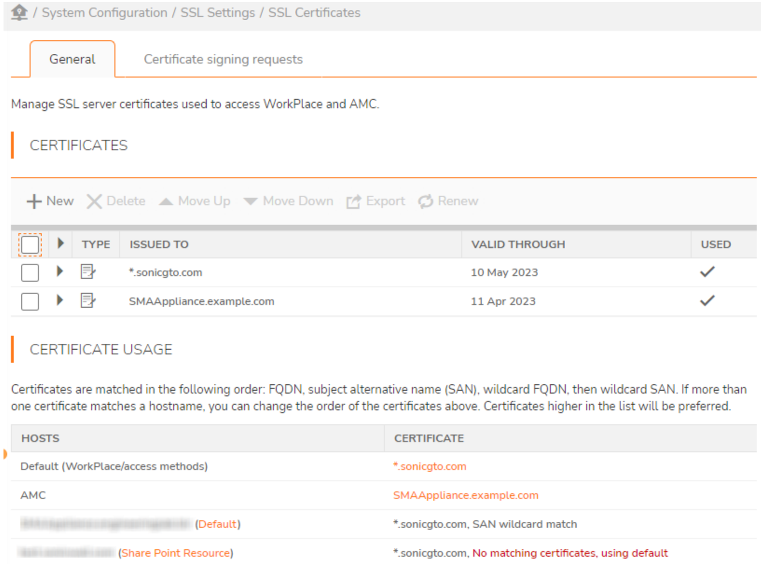
[redacted] (self-signed)
Valid through: 26 Mar 2024

Virtual hosting certificates for WorkPlace sites and URL resources

[redacted]

2. In the **SSL Certificates** section, click **Edit**.

The **SSL Certificates** page displays.



/ System Configuration / SSL Settings / SSL Certificates

General | Certificate signing requests

Manage SSL server certificates used to access WorkPlace and AMC.

CERTIFICATES

+ New ✕ Delete ▲ Move Up ▼ Move Down Export Renew

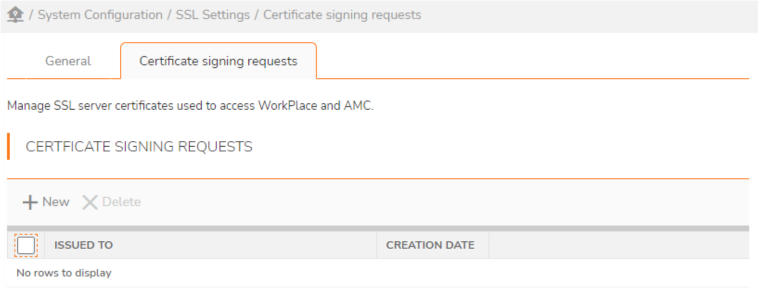
□		TYPE	ISSUED TO	VALID THROUGH	USED
□	▸		*.sonicgto.com	10 May 2023	✓
□	▸		SMAAppliance.example.com	11 Apr 2023	✓

CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	*.sonicgto.com
AMC	SMAAppliance.example.com
[redacted] (Default)	*.sonicgto.com, SAN wildcard match
[redacted] (Share Point Resource)	*.sonicgto.com, No matching certificates, using default

3. Click the **Certificate signing requests** tab.



/ System Configuration / SSL Settings / Certificate signing requests

General | Certificate signing requests

Manage SSL server certificates used to access WorkPlace and AMC.

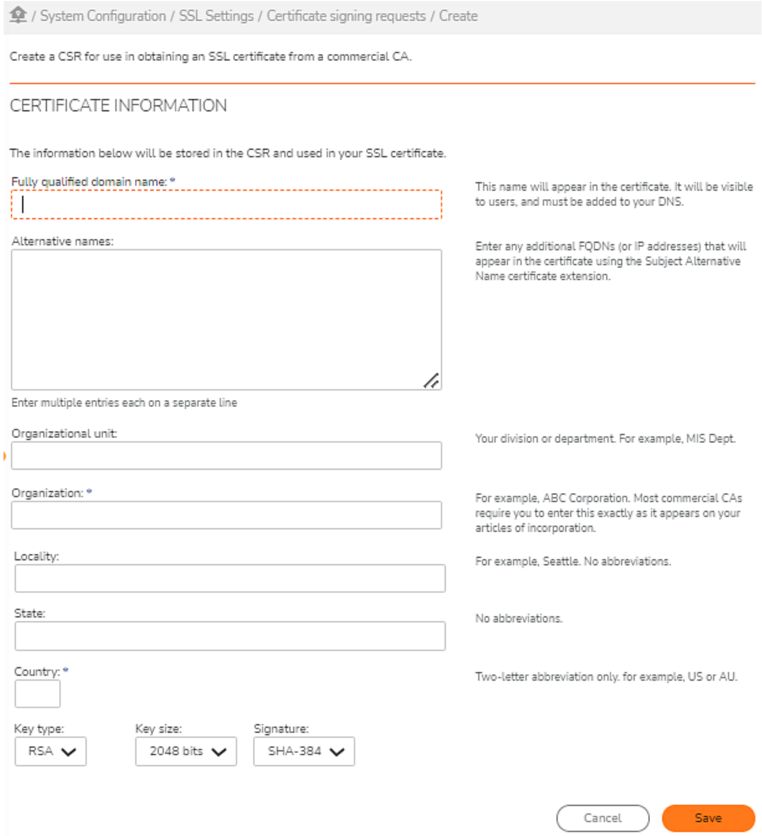
CERTFICATE SIGNING REQUESTS

+ New ✕ Delete

□	ISSUED TO	CREATION DATE
No rows to display		

4. In the **Certificate Signing Requests** area, click the **+** (New) icon.

The **Create Certificate Signing Request** page displays.



/ System Configuration / SSL Settings / Certificate signing requests / Create

Create a CSR for use in obtaining an SSL certificate from a commercial CA.

CERTIFICATE INFORMATION

The information below will be stored in the CSR and used in your SSL certificate.

Fully qualified domain name: * — This name will appear in the certificate. It will be visible to users, and must be added to your DNS.

Alternative names: — Enter any additional FQDNs (or IP addresses) that will appear in the certificate using the Subject Alternative Name certificate extension.

Enter multiple entries each on a separate line

Organizational unit: — Your division or department. For example, MIS Dept.

Organization: * — For example, ABC Corporation. Most commercial CAs require you to enter this exactly as it appears on your articles of incorporation.

Locality: — For example, Seattle. No abbreviations.

State: — No abbreviations.

Country: * — Two-letter abbreviation only. for example, US or AU.

Key type: RSA

Key size: 2048 bits

Signature: SHA-384

5. The Certificate information you fill out is stored in the CSR and used by the commercial CA when generating your certificate; it may be visible to users who connect to the appliance.

   ⓘ **NOTE:** Some commercial CAs may have problems reading CSRs that contain characters produced by pressing the SHIFT key, such as & or !. For example, when specifying your company name or other information, you may want to spell out & (if used) as *and*.

   a. In the **Fully qualified domain name** field, type the server name as you want it to appear in the certificate. Also known as a common name (or CN), this is usually composed of a host and a domain name; for example, you might type `vpn.example.com`.

      Users with a Web-based client will use this name to access the appliance (in other words, to access WorkPlace), so it's best to use a name that is easily remembered. You'll also reference this name when configuring the Connect or OnDemand components to provide access to TCP/IP resources. You must add this name to your external DNS to make the appliance accessible to users.

      Certificate Signing Requests can be created with multiple FQDN or IP addresses. On the **SSL Settings > SSL Certificate > Create Certificate Signing Request** page, simply enter multiple FQDNs and/or IP addresses separated by commas. Any number of SANs can be added to a certificate, but the text input field is 1,000 characters maximum. Wild cards are permitted. The entered FQDNs and IP addresses are encoded in the subject alternative name certificate extension and the certificate FQDN is encoded as an additional SAN entry in the CSR.

b. In the **Alternative name** field, type any additional FQDNs or IP addresses that should appear in the certificate using the Subject Alternative Name certificate extension. Enter multiple entries each on a separate line.

c. In the **Organizational unit** field, type your division or department (for example, MIS Dept).

d. In the **Organization** field, type your company or organization name as you want it to appear in your SSL certificate.

e. In the **Locality** field, type your city or town. Do not use an abbreviation.

f. In the **State** field, type the name of your state or province. Do not use an abbreviation.

g. In the **Country** field, type the two-letter abbreviation for your country. For a list of valid country codes, see the International Organization for Standardization (ISO) Web site at http://www.iso.org and search for ISO 3166-1.

h. In the **Key length** drop-down menu, select the key length you want to use for the key: **2048** (the default), **3072**, or **4096**. Larger keys increase security.

6. Select the key type from the **Key type** drop-down menu.

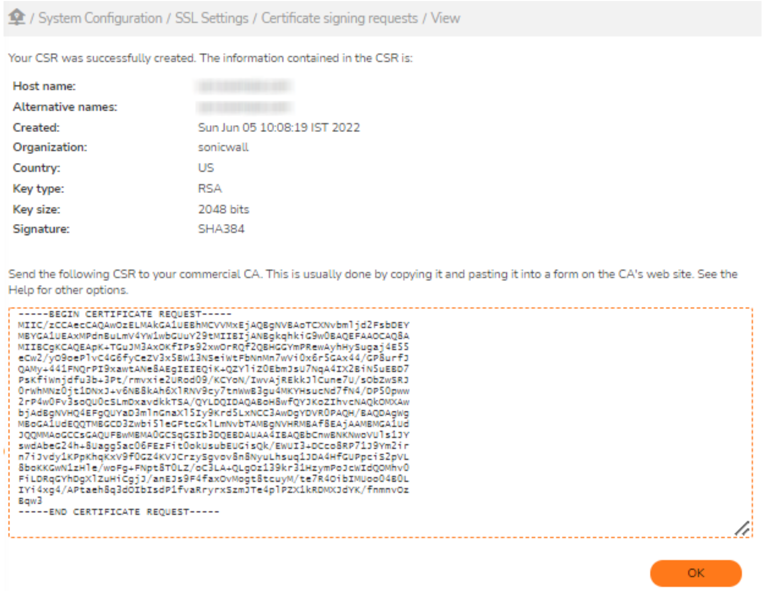
   The default is **RSA**.

7. In the **Signature** drop-down menu, select the algorithm used for the certificate.

8. Review the information to verify that you've typed it correctly.

9. Click **Save** to generate the CSR.

   The **Certificate Signing Request** page redisplays with the CSR information you entered.



/ System Configuration / SSL Settings / Certificate signing requests / View

Your CSR was successfully created. The information contained in the CSR is:

Host name:	[redacted]
Alternative names:	[redacted]
Created:	Sun Jun 05 10:08:19 IST 2022
Organization:	sonicwall
Country:	US
Key type:	RSA
Key size:	2048 bits
Signature:	SHA384

Send the following CSR to your commercial CA. This is usually done by copying it and pasting it into a form on the CA's web site. See the Help for other options.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC/zCCAecCAQAwOzELMAkGA1UEBhMCVVMxEjAQBgNVBAoTCXNvbmljd2FsbDEY
MBYGA1UEAxMPdnBuLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEApK+TGuJM3AxOKfIPs92xwOrRQf2QBHGGYmPRewAyhHySugaj4E55
eCw2/yO9oePlvC4G6fyCeZV3x5BW13NSeiWtFbNnMn7wVi0x6r5GAx44/GP8urfJ
QAMy+441FNQrPI9xawtANe8AEgIEIEQiK+QZYliZ0EbmJsU7NqA4IX2BiN5uEBD7
PsKfiWnjdfu3b+3Pt/rmvxie2URod09/KCYoN/IwvAjREkkJlCune7U/sObZwSRJ
0rWhMNz0jt1DNxJ+v6NB8kAh6XlRNV9cy7tnWwB3gu4MKYHsucNd7fN4/DP50pww
2rP4w0Fv3soQU0cSLmDxavdkkTSA/QYLDQIDAQABoH8wfQYJKoZIhvcNAQkOMXAw
bjAdBgNVHQ4EFgQUYaD3mlnGnaXl5Iy9Krd5LxNCC3AwDgYDVR0PAQH/BAQDAgWg
MBoGA1UdEQQTMBGCD3Zwbi5leGFtcGxlLmNvbTAMBgNVHRMBAf8EAjAAMBMGA1Ud
JQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBDAUAA4IBAQBbCnwBNKNwoVUls1JY
swdAbeG24h+8Uagg5ac06FEzFit0okUsubEUGisQk/EWUI3+DCco8RP71J9Ym2ir
n7iJvdy1KPpKhqKxV9f0GZ4KVJCrzySgvov8n8NyuLhsuq1JDA4HfGUPpciS2pVL
8boKKGwN1zHle/woFg+FNpt8T0LZ/oC3LA+QLgOz139kr31HzymPoJcWIdQOMhv0
FiLDRqGYhDgXlZuHiCgjJ/anEJs9F4faxOvMogt8tcuyM/te7R4OibIMUoo04B0L
IYi4xg4/APtaeh8q3dOIbIsdP1fvaRryrxSzmJTe4plPZX1kRDMXJdYK/fnmnvOz
Bqw3
-----END CERTIFICATE REQUEST-----
```

10. Copy the contents of the CSR text from AMC to the clipboard or into a text file.

11. Click **OK**.

Step 2: Submit the CSR to a Commercial CA

The process of submitting a CSR varies, depending on which commercial CA you choose.

To submit a CSR to a commercial CA:

1. Copy the contents of your certificate signing request from the **Create Certificate Signing Request** page in AMC.
2. Submit it to the CA using the method they request (usually you either copy and paste the CSR text into a form on the CA's Web site, or attach it to an email message).

   Depending on what is specified by the CA, you may need to paste all the text, or only the text between the `BEGIN NEW CERTIFICATE REQUEST and END NEW CERTIFICATE REQUEST` banners (including the banners themselves). If you're not sure, contact the CA.
3. Wait for the commercial CA to verify your identity. You may be asked to produce one or more documents attesting to your corporate identity (such as a business license or article of incorporation).

   ⓘ | **NOTE:** Submit your CSR only once; you may otherwise be billed twice by the CA. This would also change the internal private key, making the response from the CA unusable.

Step 3: Review CSR Response and Add CA's Root Certificate

After you've submitted your CSR, you must wait for the CA to verify your identity. After they complete this process, the CA will send you the certificate reply. It is usually in one of two formats:

- **A file attached to an email message**. In this case, you can save the file to your local file system (the one from which you'll access AMC) and then import it into AMC.
- **Text embedded within an email message**. In this case, you copy the text and paste it into a text box provided in AMC. Be sure to include the `BEGIN CERTIFICATE` and `END CERTIFICATE` banners.

If the CA does not provide a full certificate chain in the CSR response (a common practice), AMC will try to complete the certificate chain when you import the CSR response. If it is unable to complete the chain, AMC displays an error message. If this occurs, you must upload the CA's root certificate or any intermediary public certificates to the appliance. If you are acting as your own CA, you will probably need to perform this step.

To complete a certificate chain:

1. Obtain the trusted root certificate or intermediary public certificate from the CA. Most external commercial CAs provide the certificates on their Web site; if the CA is run by your company, check with the server administrator.
2. In the AMC, navigate to **System Configuration > SSL Settings**.
3. In the **SSL Certificates** area, click **Edit**.
4. In the **Certificate signing requests** list, click the **Process CSR response** link for the appropriate certificate.

   The **Import CSR Certificate page** displays.
5. Upload the certificate:

   ⓘ | **NOTE:** The format of the CA certificate required is "Apache Server".

- If the certificate is in binary format:
    1. Select **Certificate file**.
    2. Click **Browse** and then upload the certificate reply from your local file system (the computer from which you've logged in to AMC).
- If the certificate is in base-64 encoded (PEM) text format:
    1. Select **Certificate text**.
    2. Paste the certificate into the field.

       ⓘ **IMPORTANT:** Be sure to include the `BEGIN CERTIFICATE` and `END CERTIFICATE`banners.

6. Click **Save**.
7. To verify that the certificate was properly uploaded:
    a. Navigate to **System Configuration > SSL Settings > CA Certificates**.
    b. Click Edit next to **<NNN> certificates**.
    c. The new certificate should appear in the list on the **CA Certificates** page.

Step 4: Import the CSR Response Into AMC

To create a certificate, import the CSR response into AMC.

To import a certificate reply:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **SSL certificates** area, click **Edit**.
3. In the **Certificate signing requests** list, click the **Process CSR response** link for the appropriate certificate.
4. Upload the certificate:
    - If the certificate is in binary format:
        1. Select **Certificate file**.
        2. Click **Browse** and then upload the certificate reply from your local file system (the computer from which you've logged in to AMC).
    - If the certificate is in base-64 encoded (PEM) text format:
        1. Select **Certificate text**.
        2. Paste the certificate into the field.

           ⓘ **IMPORTANT:** Be sure to include the `BEGIN CERTIFICATE` and `END CERTIFICATE`banners.
5. In the **Used by** drop-down menu, select **AMC** or **WorkPlace/access methods** (or select **None** if you want to build a list of certificates from which to choose later). If you defined additional WorkPlace sites (in addition to the default WorkPlace site), their names are included in this list.
6. Click **Save**.

7. To verify that the certificate was properly uploaded, click the plus sign (**+**) next to it on the **SSL Certificates** page.

Step 5: Apply Your Changes

To start using a new certificate, you need to apply your configuration changes. For more information, see Applying Configuration Changes.

After applying the change, the appliance examines the new certificate and begins using it for all new connections. If the appliance fails to correctly process the certificate, you see a failure message and the event log records information about the failure. Typically, this occurs if there is no certificate, the certificate has expired (or is not yet valid), or the cached password in the encrypted password file is incorrect.

ⓘ **NOTE:** If your users authenticate using digital certificates, you must configure a trusted root file on the server as well as on the clients. See Configuring Client Certificate Revocation.

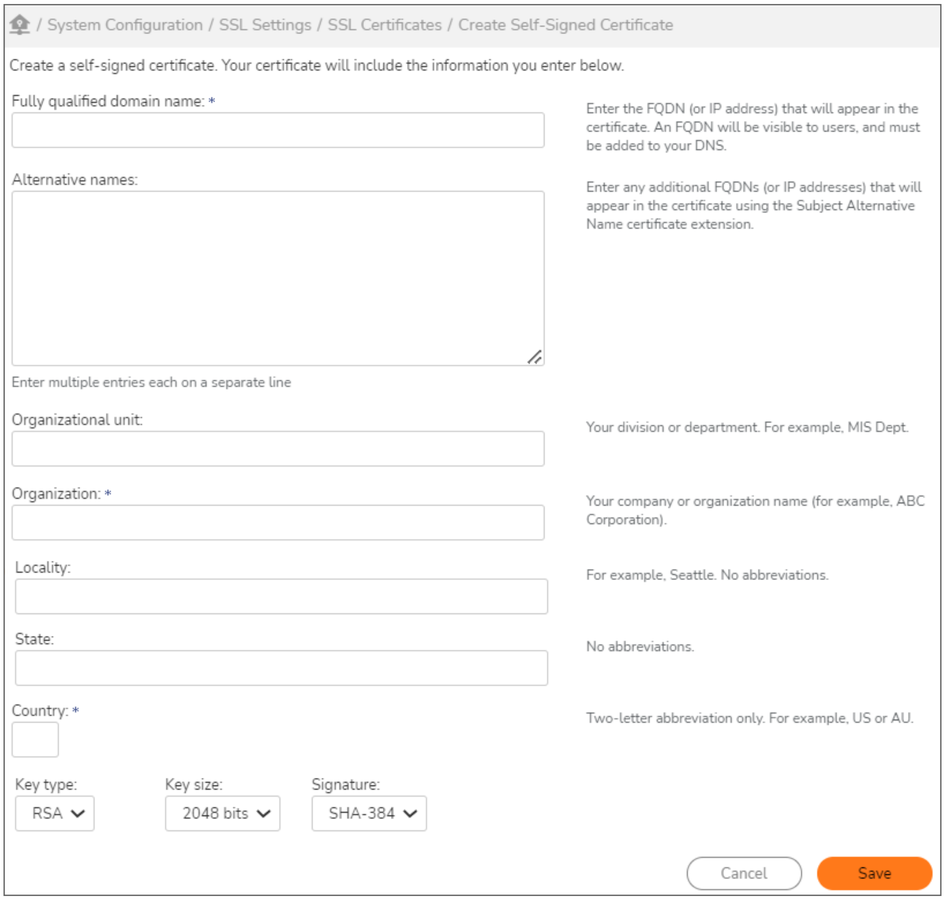
Creating a Self-Signed Certificate

If you plan to use a self-signed SSL certificate (instead of obtaining a certificate from a commercial CA), you can create one using AMC. A host is not selected for the certificate, because there is no one to one mapping of certificates to hosts. Wildcard certificates allow one certificate to map to multiple hosts. In addition, a self-signed SSL certificate can be created with multiple FQDN or IP addresses.

ⓘ **NOTE:** You can use self-signed SSL certificate only in testing or evaluation systems.

To create a self-signed certificate:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **SSL Certificates** area, click **Edit**.
3. Click the **+** (New) icon.
4. Select **Create self-signed certificate** from the menu.



/ System Configuration / SSL Settings / SSL Certificates / Create Self-Signed Certificate

Create a self-signed certificate. Your certificate will include the information you enter below.

Fully qualified domain name: *

Enter the FQDN (or IP address) that will appear in the certificate. An FQDN will be visible to users, and must be added to your DNS.

Alternative names:

Enter any additional FQDNs (or IP addresses) that will appear in the certificate using the Subject Alternative Name certificate extension.

Enter multiple entries each on a separate line

Organizational unit:

Your division or department. For example, MIS Dept.

Organization: *

Your company or organization name (for example, ABC Corporation).

Locality:

For example, Seattle. No abbreviations.

State:

No abbreviations.

Country: *

Two-letter abbreviation only. For example, US or AU.

Key type: RSA

Key size: 2048 bits

Signature: SHA-384

5. In the **Fully qualified domain name** field, type a wildcard domain name such as `*.domainname.com`, or type the individual server name as you want it to appear in the certificate:

    - The main appliance certificate can be a wildcard certificate, or you might type something like `vpn.example.com`. You must add this name to your external DNS to make the appliance accessible to users.

      This is the name users will enter for access to Web-based resources on your network. For a wildcard certificate, the * matches any string of characters up to the dot, such as specific server names. You also reference this name when configuring the Connect clients to provide access to TCP/IP resources.

    - If this certificate will be used by AMC (as opposed to WorkPlace), you might type something like `amc.example.com`. In most cases, you should add this name to your internal DNS to simplify access to AMC.

    - Any number of SANs can be added to a certificate, but the text input field is 1,000 characters maximum. Simply enter multiple FQDNs and/or IPv4 or IPv6 addresses separated by commas. SANs can contain wildcard entries (`*.example.com, *.access.example.com`), unique FQDNs (`access.example.com, vpn.example.com`), and IP addresses.

The entered FQDNs and IP addresses are encoded in the subject alternative name certificate extension and FQDNs are encoded as an additional SAN name in the certificate. If a SAN is an IP address, it is encoded as an IPAddress in the SAN extension instead of a DNSName.

6. In the **Alternative names** field, type any additional FQDNs or IP addresses that should appear in the certificate using the Subject Alternative Name certificate extension. Separate multiple alternative names and IP addresses with a comma.
7. In the **Organization** field, type the company or organization name as you want it to appear in your SSL certificate.
8. In the **Country** field, type the two-letter abbreviation for your country. For a list of valid country codes, go to the International Organization for Standardization (ISO) Web site at http://www.iso.org and look for information on ISO 3166-1.
9. In the **Key size** list, select the key length you want to use for the key. Larger keys increase security.
10. In the **Signature** list, select the algorithm used for the certificate.
11. Click **Save**.
12. Click **Pending changes** and then apply the changes. (For more information, see Applying Configuration Changes.)

Managing Server Certificates in AMC

Topics:

- Importing an Existing Certificate from Another Computer
- Exporting an SSL Certificate

Importing an Existing Certificate from Another Computer

If you already have a certificate from a commercial CA, you may want to transfer it and its private key to the appliance. After you import the certificate, it will be used by the servers to secure user traffic on the appliance.

The appliance stores certificates in the PKCS #12 format. If your certificate is stored in a different format, convert it to PKCS #12 before importing. After performing the conversion, confirm that the PKCS #12 file contains the complete certificate chain.

To transfer an existing certificate to the appliance:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **SSL Certificates** section, click **Edit**.
3. Click the **+** (New) icon, and then select **Import certificate** from the menu.
4. On the **Import Certificate** page, click **Browse**, and then upload the certificate from your local file system (the computer from which you have logged in to AMC).
5. In the **Password** field, type the password that was used to encrypt the private key.
6. Click **Save**.
   The appliance uses the previous certificate until you apply your configuration changes.

Exporting an SSL Certificate

You can export the SSL certificate used to secure user traffic on the appliance. The certificate will include the private key and be saved in PKCS #12 format.

To export the SSL certificate from the appliance:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **SSL Certificates** section, click **Edit**.
3. Select the checkbox next to the certificate you want to export, and then click the **Export** icon.

   The **Export Certificate page** displays.
4. In the **Password** field, type the password that you want to use to encrypt the private key.
5. Click **Save**.
6. Download the certificate file to your local file system (the computer from which you've logged into AMC).
7. Click **OK**.

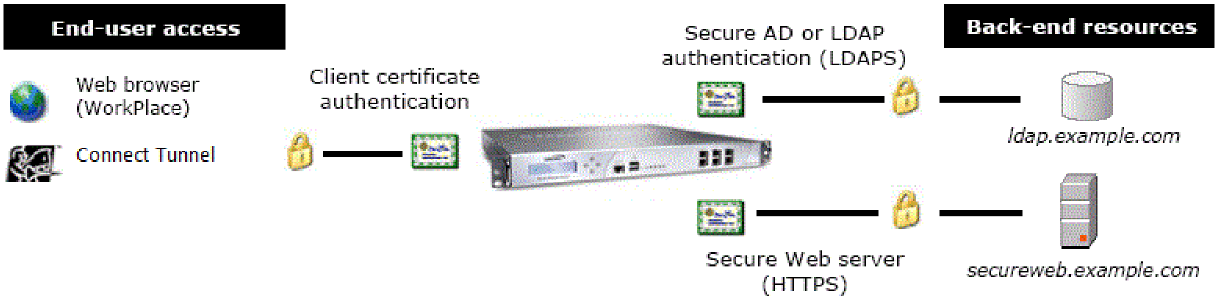
CA Certificates

Every CA requires a certificate so that it can be "trusted" by entities that request digital certificates from it. If a client trusts a CA certificate, it automatically trusts any other certificates that are issued by that CA. CA certificates thus form one of the foundations of public key cryptography. The CA certificate is either signed by the CA itself (a "root certificate"), or by a higher authority in a hierarchy of CAs in a public key infrastructure (an "intermediate CA certificate").

The appliance uses CA certificates to secure the following:

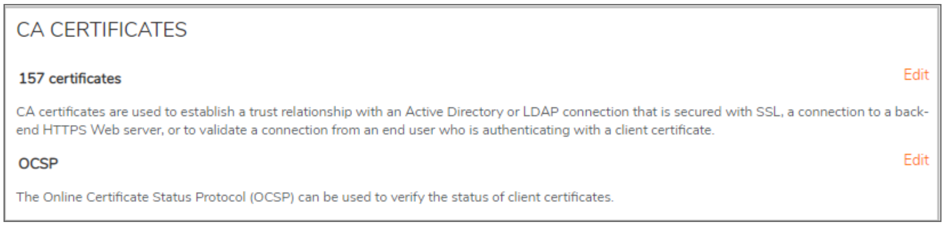
- Connections to a back-end LDAP or AD authentication server
- Connections to a back-end HTTPS Web server
- Device profiling (End Point Control), to verify the validity of certificates submitted by users who connect to the appliance. See the Device Profile Attributes: client certificate table in Device Profile Attributes for more information.

CA Certificates Usage



The appliance includes over 100 public root certificates from leading commercial CAs. If you've obtained a certificate from a commercial CA, its root certificate or intermediary public certificate is probably already installed on the appliance. However, if you are acting as your own CA you must import a root or intermediary public certificate to the appliance.

To view the list of certificates, click **Edit** in the **CA Certificates** area of the **SSL Settings** page.



CA CERTIFICATES

157 certificates

Edit

CA certificates are used to establish a trust relationship with an Active Directory or LDAP connection that is secured with SSL, a connection to a back-end HTTPS Web server, or to validate a connection from an end user who is authenticating with a client certificate.

OCSP

Edit

The Online Certificate Status Protocol (OCSP) can be used to verify the status of client certificates.

This is also where you delete CA certificates.

Topics:

- Importing CA Certificates
- Configuring Local CA in AMC
- Configuring Client Certificate Revocation
- Managing CA Certificates

Importing CA Certificates

If the appliance is not configured with the necessary CA certificate, you must obtain a copy and import it to the appliance using AMC. The procedure is the same, whether the certificate will be used to secure connections to back-end resources, or to authenticate users by means of a client certificate.

The new certificate appears in the alphabetical list on the **CA Certificates** page. When you upload a CA certificate for use with client certificate authentication (and you apply the change), network services are automatically restarted and user connections are terminated, forcing users to reauthenticate. You may want to schedule the change during off-peak hours.

ⓘ | **NOTE:**

- If the certificate is being used to secure authentication server connections, check to see that the appropriate **LDAP over SSL** or **Active Directory over SSL** settings are enabled on the **Configure Authentication Server** page in AMC.
- By default, the Web proxy service is configured to verify the root certificate presented by back-end HTTPS Web servers. This important security check helps ensure that you can trust the identity of the back-end server. See Configuring the Web Proxy Service.
- If you do not want to trust a CA listed on the **CA Certificates** page, select the checkbox next to it, and then click **Delete**.
- When setting up devices profiles, avoid checking for client certificates within the same zone more than three times.

To import a CA certificate to the appliance:

1. Obtain the trusted root certificate or intermediary public certificate from the CA. Most external commercial CAs provide the certificates on their Web sites; if the CA is run by your company, check with the server administrator.
2. In the AMC, navigate to **System Configuration > SSL Settings**.
3. In the **CA Certificates** section, click **Edit** on the ***NNN*** **certificates** line.
4. Click the **+** (New) icon.

   The **Import CA Certificate** page displays.
5. Do one of the following:
   - If the certificate is in binary format:
     1. Select **Certificate file**.
     2. Click **Browse** and then upload the certificate reply from your local file system (the computer from which you've logged in to AMC).
   - If the certificate is in base-64 encoded (PEM) text format:
     1. Select **Certificate text**.
     2. Paste the certificate into the field.

        ⓘ **IMPORTANT:** Be sure to include the `BEGIN CERTIFICATE` and `END CERTIFICATE` banners.
6. Specify the connection types this certificate will be used to secure:

   Connection Types For Certificates

Connection type	Description
Authentication server connections (LDAPS)	Securing your LDAP or Active Directory (AD) connection with SSL enhances security by preventing attempts to impersonate the LDAP or AD server. To configure LDAP or AD over SSL, you must add the root certificate for the CA that granted your LDAP or AD certificate to the SSL trusted roots file.
Web server connections (HTTPS)	If you have a back-end Web resource that is secured with SSL (that is, it uses HTTPS instead of HTTP), configure the Web proxy service to verify the root certificate presented by the back-end server. This important security check will help ensure that you can trust the identity of the back-end server. See Configuring the Web Proxy Service for details. If the back-end server's root certificate is not pre-installed on the appliance, you must obtain a copy and import it in AMC.

Device profiling (End Point Control)	EPC can be used to verify the validity of certificates submitted by users who connect to the appliance. If a client certificate is used in a device profile to classify users into an EPC zone, the appliance must be configured with the root or intermediary certificates for the CA that issued the client certificate to your users. When the appliance interrogates the user's computer to determine if the specified certificate is present, it can be configured to search just the system store (*HKLM\SOFTWARE\Microsoft\SystemCertificates*), or also include the user store (*HKCU\Software\Microsoft\SystemCertificates*).
OCSP response verification	The OCSP response signing certificate is used to verify a response from a configured OCSP responder. When importing the OCSP response signing certificate, enable **OCSP response verification**. This is a different certificate than the CA certificate for the OCSP responder or server itself, which is used in the PKI Authentication server.
SAML message verification	The SAML message verification is used to verify the SAML messages.

7. Click **Import**.

   The **CA Certificates page** displays and displays a confirmation message.

Configuring Client Certificate Revocation

Certificates installed on client devices can be used to authenticate users or devices, giving them access to a particular realm. A certificate is usually valid until it expires, but it is possible for it to be compromised before it expires. For example, a CA may decide that a certificate was improperly issued, or its private key may have been compromised.

You can consult a certificate revocation list (CRL) to check a certificate's validity (its location—the CRL distribution point, or CDP—is typically included in the X.509 certificate). If a certificate is no longer valid, the user is denied access. CRLs are published for each authority and can contain status of only the certificates issued by that certificate authority. This requires a separate, hierarchical CRL server for each CA that you want to trust. The client needs to know the public key for each CA in the chain to verify each certificate and CA at each level in the chain.

Online Certificate Status Protocol (OCSP) and an OCSP responder server can be used instead of a CRL server to check the status of a certificate. OCSP responders take the certificate from a client, evaluate it and give back a response to the server as revoked, unrevoked, or unknown. OCSP can save bandwidth in a large organization, as the CRL server list can get very large. OCSPs can be configured to operate for any number of CAs and certificates. A single OCSP server can be configured for the entire PKI infrastructure, irrespective of CA relations.

ⓘ | **NOTE:**

- If both CRL and OCSP are enabled for a CA certificate, only OCSP will be used.
- Fallback from CRL to OCSP or OCSP to CRL is not supported.

Topics:

- Managing Certificates with a CRL
- Configuring an OCSP Responder

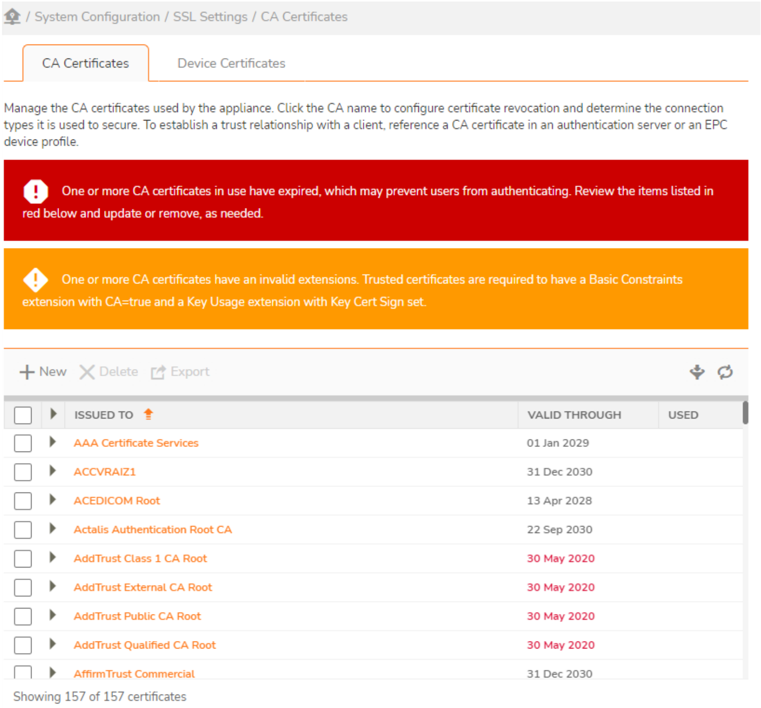
Managing Certificates with a CRL

Use the **Manage CA Certificate** page in AMC to configure certificate revocation checking for individual certificates, and determine the connection types the certificate is used to secure.

To verify the validity of a client certificate and configure certificate revocation:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. Under **CA Certificates**, click **Edit** on the ***NNN*** **certificates** line.

   All of the installed certificates are displayed.



Manage the CA certificates used by the appliance. Click the CA name to configure certificate revocation and determine the connection types it is used to secure. To establish a trust relationship with a client, reference a CA certificate in an authentication server or an EPC device profile.

One or more CA certificates in use have expired, which may prevent users from authenticating. Review the items listed in red below and update or remove, as needed.

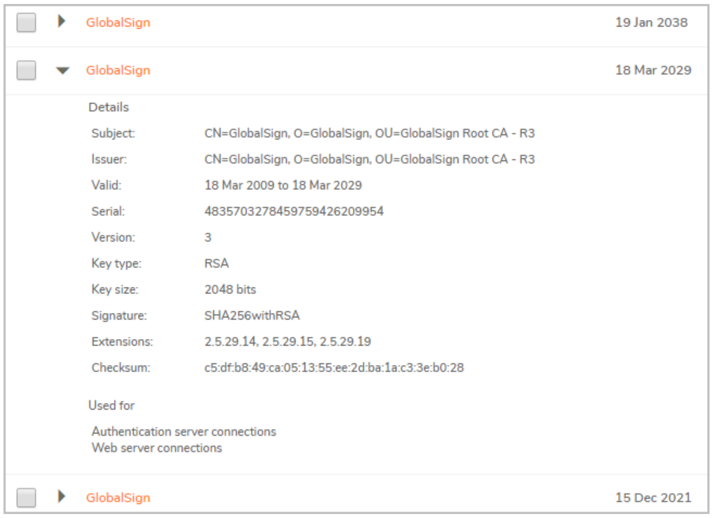
One or more CA certificates have an invalid extensions. Trusted certificates are required to have a Basic Constraints extension with CA=true and a Key Usage extension with Key Cert Sign set.

□	▶	ISSUED TO	VALID THROUGH	USED
□	▶	AAA Certificate Services	01 Jan 2029	
□	▶	ACCVRAIZ1	31 Dec 2030	
□	▶	ACEDICOM Root	13 Apr 2028	
□	▶	Actalis Authentication Root CA	22 Sep 2030	
□	▶	AddTrust Class 1 CA Root	30 May 2020	
□	▶	AddTrust External CA Root	30 May 2020	
□	▶	AddTrust Public CA Root	30 May 2020	
□	▶	AddTrust Qualified CA Root	30 May 2020	
□	▶	AffirmTrust Commercial	31 Dec 2030	

Showing 157 of 157 certificates

3. To see details about a certificate, click the right arrow (▶) in the second column. To edit a certificate, click its link. For example:

a. Click the right arrow (▶) next to a **GlobalSign** certificate to see its details.



□ ▶ GlobalSign 19 Jan 2038

□ ▼ GlobalSign 18 Mar 2029

Details

Subject:	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
Issuer:	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
Valid:	18 Mar 2009 to 18 Mar 2029
Serial:	4835703278459759426209954
Version:	3
Key type:	RSA
Key size:	2048 bits
Signature:	SHA256withRSA
Extensions:	2.5.29.14, 2.5.29.15, 2.5.29.19
Checksum:	c5:df:b8:49:ca:05:13:55:ee:2d:ba:1a:c3:3e:b0:28

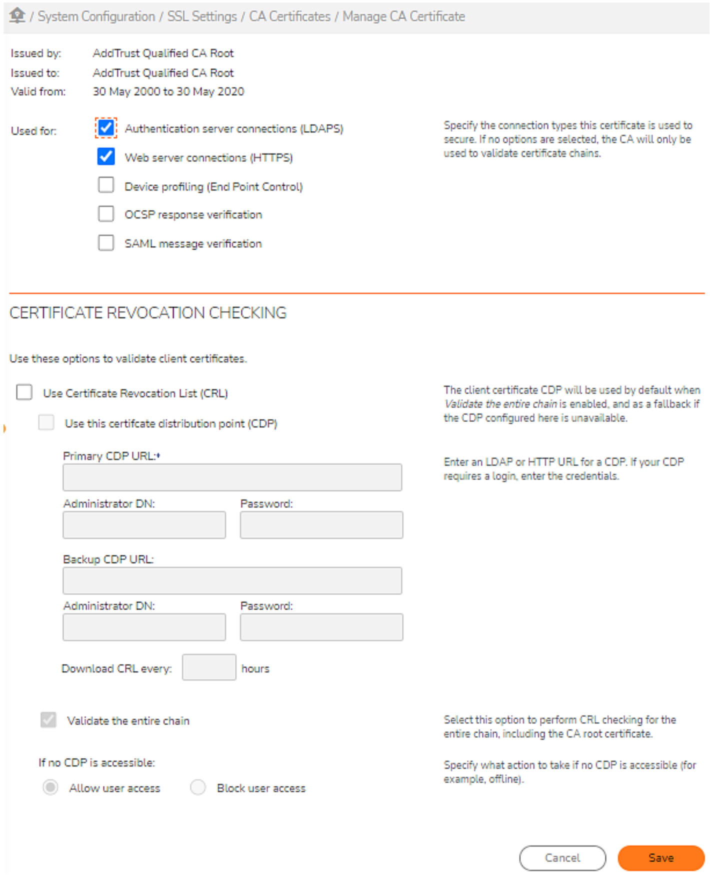
Used for

Authentication server connections
Web server connections

□ ▶ GlobalSign 15 Dec 2021

b. Click the link to edit it.

The **Manage CA Certificate** page displays.



/ System Configuration / SSL Settings / CA Certificates / Manage CA Certificate

Issued by: AddTrust Qualified CA Root

Issued to: AddTrust Qualified CA Root

Valid from: 30 May 2000 to 30 May 2020

Used for:

- ☑ Authentication server connections (LDAPS)
- ☑ Web server connections (HTTPS)
- □ Device profiling (End Point Control)
- □ OCSP response verification
- □ SAML message verification

Specify the connection types this certificate is used to secure. If no options are selected, the CA will only be used to validate certificate chains.

CERTIFICATE REVOCATION CHECKING

Use these options to validate client certificates.

□ Use Certificate Revocation List (CRL)

□ Use this certifcate distribution point (CDP)

The client certificate CDP will be used by default when *Validate the entire chain* is enabled, and as a fallback if the CDP configured here is unavailable.

Primary CDP URL:*

Administrator DN: Password:

Enter an LDAP or HTTP URL for a CDP. If your CDP requires a login, enter the credentials.

Backup CDP URL:

Administrator DN: Password:

Download CRL every: hours

☑ Validate the entire chain

Select this option to perform CRL checking for the entire chain, including the CA root certificate.

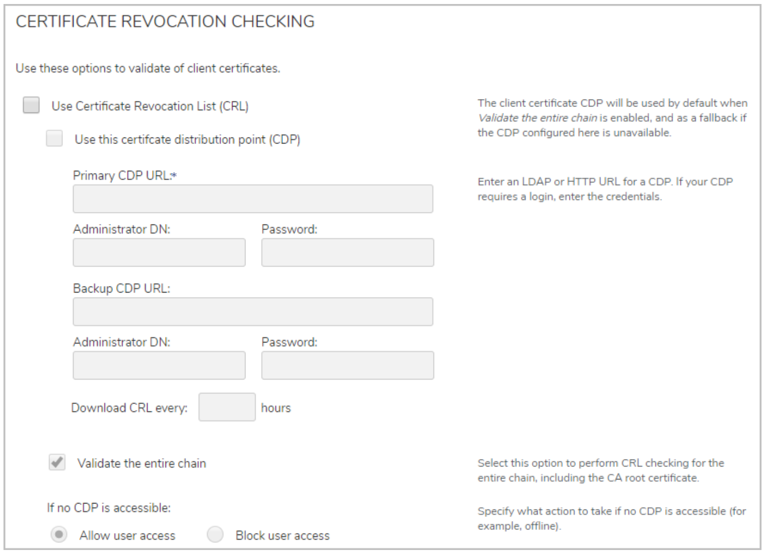
If no CDP is accessible:

● Allow user access ○ Block user access

Specify what action to take if no CDP is accessible (for example, offline).

4. In the **Used for** area, specify the connection types this certificate is used to secure.
   - **Authentication server connections (LDAPS)**—See Configuring a PKI Authentication Server.
   - **Web server connections (HTTPS)**-See CA Certificates.
   - **Device profiling (End Point Control)**-See the Device Profile Attributes: client certificate table in Device Profile Attributes.
   - **OCSP response verification** - Verifies a response from a configured OCSP responder.
   - **SAML message verification**- Verifies a SAML message.
5. To specify CRL settings, check the **Use Certificate revocation list** in the **Certificate revocation checking** area.

   ⓘ **IMPORTANT:** The format for the CRL must be DER-based (`.crl`); the appliance cannot use a CRL that's been created in PEM format.



CERTIFICATE REVOCATION CHECKING

Use these options to validate of client certificates.

□ Use Certificate Revocation List (CRL)

The client certificate CDP will be used by default when *Validate the entire chain* is enabled, and as a fallback if the CDP configured here is unavailable.

□ Use this certifcate distribution point (CDP)

Primary CDP URL:*

Enter an LDAP or HTTP URL for a CDP. If your CDP requires a login, enter the credentials.

Administrator DN:

Password:

Backup CDP URL:

Administrator DN:

Password:

Download CRL every: hours

☑ Validate the entire chain

Select this option to perform CRL checking for the entire chain, including the CA root certificate.

If no CDP is accessible:

● Allow user access ○ Block user access

Specify what action to take if no CDP is accessible (for example, offline).

6. The appliance retrieves lists of revoked certificates from a CRL distribution point (CDP). Specify the location of this CDP:
    - The CDP is usually specified in the certificate itself. By default, the appliance uses the **CDP from the client certificate**.
    - Alternatively you can specify a URL for it. Check the **Use this certificate distribution point (CDP) checkbox**. If a login is required for it, type the credentials.
7. If **Use this certificate distribution point (CDP)** is selected, you can specify how often the CRL should be retrieved using the **Download CRL every <n> hours** option. If you don’t specify a download interval, a new CRL is retrieved when the old one expires. (CRLs are updated frequently so that when a certificate is revoked, that information is distributed in a timely manner).
8. The appliance checks client certificates against this list. To perform CRL checking for the entire chain of certificates, starting with the CA root certificate, select the **Validate the entire chain** checkbox.
9. Specify whether users should be allowed or denied access if the CDP is inaccessible by selecting **Allow user access** or **Block user access**. The remote CDP you specified might be offline, or it may not be indicated on the certificate. (It is an optional item for the X.509 standard, not a mandatory one.)
10. Click **Save**.

Configuring an OCSP Responder

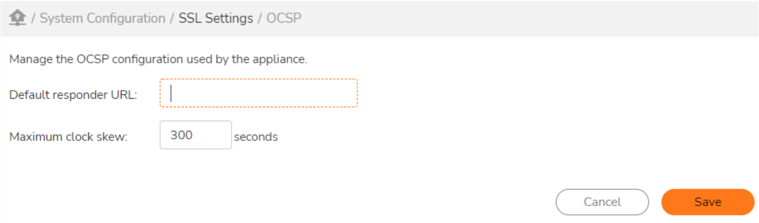
Use the **OCSP** page in AMC to configure global settings for an OCSP responder. The OCSP responder can be referenced when configuring a PKI authentication server.

ⓘ **NOTE:** Just importing a CA certificate and enabling OCSP is not sufficient for OCSP to work. You must import the OCSP response signing certificate for the CA certificate being used and enable OCSP response verification when importing it. See Importing CA Certificates.

To configure an OCSP responder:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **CA Certificates** section, on the **OCSP** line, click **Edit**.

   The **OCSP** page displays.



/ System Configuration / SSL Settings / OCSP

Manage the OCSP configuration used by the appliance.

Default responder URL:

Maximum clock skew: 300 seconds

3. In the **Default responder URL** field, enter the URL of the OCSP responder server.
4. In the **Maximum clock skew** field, enter the maximum number of seconds that the OCSP response time can differ from the local time. The default value is **300** seconds, the minimum is 1 second, and the maximum is 3600 seconds.
5. Click **Save**.

Managing CA Certificates

This section describes tasks related to managing certificates on the appliance; importing certificates is described in Importing CA Certificates.

Topics:

- Viewing CA Certificate Details
- Mapping Certificates to Hosts
- Exporting CA Certificates
- Deleting CA Certificates

Viewing CA Certificate Details

You can view the details for the appliance certificate, such as the subject, issuer, start and end time, serial number, and MD5 checksum. Details of a newly imported certificate are not available until you have applied the configuration change.

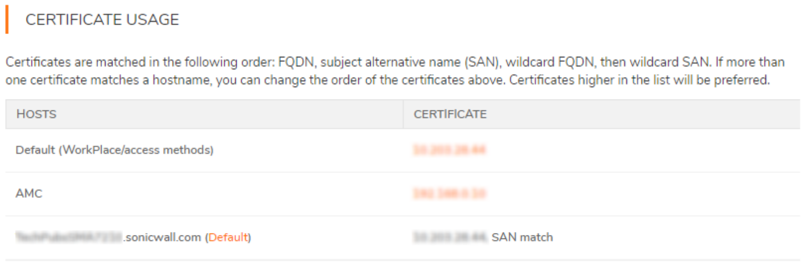
To view CA certificate details:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **CA Certificates** area, click **Edit**.
3. Click the click the right arrow (▶) to the left of the certificate you want to see details about.

Mapping Certificates to Hosts

As multiple hosts on the appliance may use a single wildcard certificate, the **Certificate usages** table provides a mapping of a single certificate to multiple sets of hosts. A set of hosts is defined as one or more WorkPlace sites, Exchange sites, or custom FQDN mapped resources that are on the same IP address. Any given set of hosts must use the same wildcard certificate and therefore are treated as a single item for mapping certificates in the **Certificate usages** table. AMC is treated as a separate host even if it is on the same IP address as other hosts on a single-homed appliance.

You can set the certificate for default and AMC host. All other host's certificate is assigned automatically and can not be changed.



CERTIFICATE USAGE

Certificates are matched in the following order: FQDN, subject alternative name (SAN), wildcard FQDN, then wildcard SAN. If more than one certificate matches a hostname, you can change the order of the certificates above. Certificates higher in the list will be preferred.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)	[redacted]
AMC	[redacted]
[redacted].sonicwall.com (Default)	[redacted] SAN match

To map a new certificate to a host or set of hosts:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **SSL Certificates** section, click **Edit**.
3. In the **Certificates** column of the **Certificate usages** table, click on the certificate to activate an in-place editor with a drop-down certificate selector.
4. Select the certificate. For individual hosts, all certificates are available for selection. For a set of multiple hosts, only wildcard certificates are available for selection.
5. Click **OK**.

Exporting CA Certificates

You can export a CA certificate to your local computer. The certificate is saved in PKCS #12 format.

To export a CA certificate:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **CA Certificates** section, on the ***NNN*** **certificates** line, click **Edit**.
3. Select the checkbox to the left of the certificate you want to export.
4. Click the **Export** icon.
5. Click **OK**.
   The certificate is saved (by default) to a file named `certauth.cert`.

Deleting CA Certificates

To make the list of certificates more manageable, you might want to delete those that you know you will never need.

To delete a CA certificate:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. In the **CA Certificates** section, on the ***NNN*** **certificates** line, click **Edit**.
3. Select the checkbox to the left of any certificates you want to delete.
4. Click the **Delete** icon.

About Intermediate Certificates

You can configure an authentication server to trust intermediate CAs without verifying the entire chain. This provides benefits, such as distributing certificate management among several signing authorities, several of whom might be remote to the root CA server and therefore would otherwise be unable to issue certificates, and adds security because the compromise of any single signing authority does not compromise the entire network.

To configure trusted intermediate certificates, see Configuring a PKI Authentication Server.

For example, you could create a root certificate signing authority on a system that is not connected to the corporate network. You can then issue a set of trusted intermediate signing authority certificates to be deployed in various sectors of the network (often by department or organizational unit). For the VPN, this is most often done to distribute machine or personal certificates to client systems.

The other alternative is to obtain a signing certificate from a certificate authority such as VeriSign or Thawte. In this case, your main CA is actually an intermediate CA itself.

By SSL rules, the root CA certificate must be accessible in order to validate the entire chain. However, the appliance makes no distinction between importing a CA certificate for trust and importing a CA certificate to validate a certificate chain for the intermediate CA that you want the appliance to trust. If no options are selected when a CA certificate is imported, the CA will only be used to validate certificate chains. (The options are the connection types the certificate is used to secure: Authentication server connections (LDAPS), Web server connections (HTTPS), and Device profiling (End Point Control)). Any CA certificate used only to validate certificate chains is not offered as a trusted signer during client certificate authentication or EPC certificate enforcement.

When an end user presents a client certificate signed by an intermediate CA, assuming the appliance trusts the signing authority, the user is allowed to authenticate and access resources normally.

When an end user presents a client certificate issued by a root CA of the trusted intermediate CA, unless the administrator has also imported the root CA for trust purposes, the end user authentication attempt fails due to lack of valid and trusted certificate.

If a client presents a certificate that is signed by a CA that exists only for chain validation, the certificate will be rejected. This results in an authentication failure or a failure for certificate authentication and in a failure to match the device profile for certificate EPC.

Working with Certificates FAQs

Topics:

- How do I Obtain a Certificate from a Non-Commercial CA?
- When do Certificates and CRLs Expire?
- Does Secure Mobile Access support SAN Certificates?
- Are Intermediate Certificates supported for End-User Certificate Verification?
- What Are the Different CA Certificates on the Appliance and How Are They Used?
- How many CA Certificates can be Stored on the Appliance?
- Can Private Keys or CSRs Generated from Other Tools be Imported to the Appliance?
- Where Is the AMC Certificate Stored?
- Should I Keep All CA Certificates on the Appliance or Just the Ones I Need?

How do I Obtain a Certificate from a Non-Commercial CA?

The process is identical to the one for obtaining a certificate from a commercial CA, except that you submit the CSR to a non-commercial CA (such as a Microsoft Self-Signed Certificate Authority). This part of the process is outlined in Step 2: Submit the CSR to a Commercial CA

When do Certificates and CRLs Expire?

Self-signed certificates are valid for one year. The expiration date for third-party certificates varies, depending on who issued the certificate; contact the CA for more information. A Certificate Revocation List (CRL) is valid for a much shorter period of time: days, or even hours.

When using certificates and CRLs, it is important for the clock on the appliance to be accurate, since it is used to determine when these items expire.

Does Secure Mobile Access support SAN Certificates?

Subject Alternative Name (SAN) certificates are supported for Workplace, Workplace sites, and Connect Tunnel. Certificates (also called UCC--Unified Communications Certificate) are used to securely encrypt communication channels between a set of clients and multiple distinct SSL or TLS services.

SAN certificates simplify the IP address/hostname/certificate sets needed for a typical deployment. With a single SAN certificate, you can utilize one IP address with multiple distinct SSL or TLS protected web or client/server services. Additionally, SANs can be used for different host names on the same IP address, alleviating the need for a one-to-one mapping of SSL certificate Common Names to FQDN.

ⓘ | **NOTE:** Only IPv4 addresses are supported in SAN certificates and Certificate Signing Requests (CSR).

Are Intermediate Certificates supported for End-User Certificate Verification?

Yes, intermediate certificates are supported for end user certificate verification. This covers PKI and LDAP certificate methods. This allows an intermediate certifying authority to be imported to validate a certificate chain, without requiring trust of the root certifying authority.

A client machine can use a client certificate that was issued by an intermediate certifying authority. When such a client certificate is imported directly on Windows 10, the client certificate is stored in the personal store, the intermediate certificate is imported to the intermediate CA store, and the root CA certificate is imported to the root CA store. This is the recommended method, and the certificates will work with tunnel clients and Workplace clients using PKI authentication. If all three certificates are stored in the personal store, which can happen if certmgr.msc is used to import the client certificate, then Connect Tunnel may display an error and deny access. This is not a recommended configuration.

What Are the Different CA Certificates on the Appliance and How Are They Used?

To see the list of CA certificates available on the appliance, click **SSL Settings** on the main navigation menu, and then click **Edit** in the **CA Certificates** area. By default, any certificate in the list can be used to secure up to three connection types (authentication server, secure Web server, and client certificate). Click on a certificate to set the connection types you want it to secure.

How many CA Certificates can be Stored on the Appliance?

The roots file can contain as many certificates as you want to trust. For instructions on how to import additional CA certificates, see Importing CA Certificates.

Can Private Keys or CSRs Generated from Other Tools be Imported to the Appliance?

Private keys and CSRs must be generated on the appliance using Setup Tool or the certificate generation tool. However, you can copy private keys and CSRs from one SMA appliance to another using the procedure described in Managing Server Certificates in AMC. Any copied certificates are overwritten if you make changes to them in AMC.

Where Is the AMC Certificate Stored?

AMC's self-signed certificate is stored on the appliance in

```
/usr/local/app/mgmt-server/datastore/active/sysconf/.
```

For AMC, a self-signed certificate is sufficient for most environments. It is important, however, to use AMC within a trusted network. Self-signed certificates protect against passive eavesdroppers but not against active attackers.

Should I Keep All CA Certificates on the Appliance or Just the Ones I Need?

For the sake of convenience, the appliance includes more than 100 CA certificates. To make your deployment more secure, you may want to pare this list down so that it includes only the CA certificates you need for client certificates, LDAPS, and HTTPS. A shorter list is also easier to manage.

Managing User Authentication

Authentication is the process of verifying a user's identity to ensure that the individual really is who he or she claims to be. (Authentication differs from authorization: it verifies identity, while authorization specifies access rights.) This section describes how to reference external authentication servers.

To manage user authentication, you must first define one or more external authentication servers in AMC, and then set up realms that reference those authentication servers. These are the realms that users will log in to. For information on realms, see Using Realms and Communities. You can also configure a local authentication repository on the appliance for testing, as described in Configuring Local User Storage.

Topics:

- About Intermediate Certificates
- Configuring Authentication Servers
- Configuring Microsoft Active Directory Servers
- Configuring LDAP and LDAPS Authentication
- Configuring RADIUS Authentication
- Integration of SMA with Cisco Duo Security MFA Server
- User-Mapped Tunnel Addressing
- Integration of SMA1000 with RSA SecurID Authentication Manager
- Configuring a PKI Authentication Server
- Additional Field for Custom Certificates
- Configuring a SAML-Based Authentication Server
- One Identity Defender
- Configuring Local User Storage
- Testing AD,LDAP,RADIUS and One Defender Authentication Configurations
- Configuring Chained Authentication
- Enabling Group Affinity Checking in a Realm
- Using One-Time Passwords for Added Security
- Configuring Personal Device Authorization

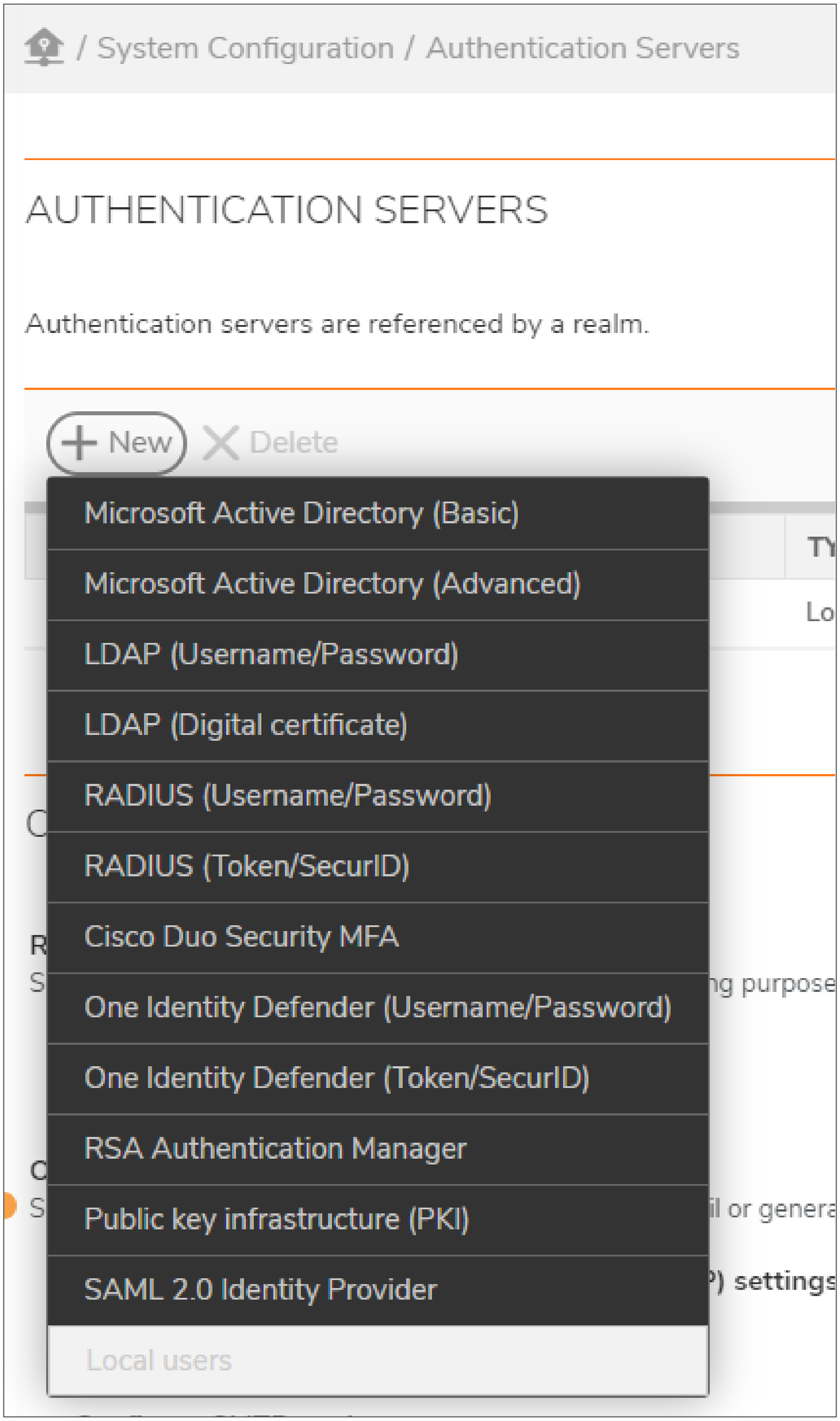
Configuring Authentication Servers

Setting up authentication involves the following: a directory (such as LDAP, Microsoft Active Directory, or the local authentication store on the appliance), an authentication method (username/password, token or smart card, or digital certificate), and other configuration items that make the authentication process unique (for example, an LDAP search base, or adding custom prompts and messages). The SMA appliance supports the leading authentication directories and methods.

After you reference an authentication server in a realm and associate users with the realm, the appliance checks users' credentials against the credentials stored in the specified authentication repository. You can also set up chained (two-factor) authentication; see Configuring Chained Authentication for details.

To configure an authentication server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

+ New
✕ Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users

3. Select the directory type or authentication method you want to configure:

Directory Type Or Authentication Method Selection

Authentication directory	Credential type	For more information
Microsoft Active Directory (Basic) Microsoft Active Directory (Advanced)	• Username/password	Configuring Microsoft Active Directory Servers
LDAP	• Username/password • Digital certificate	Configuring LDAP and LDAPS Authentication
RADIUS	• Username/password • Token-based authentication (such as SecurID or SoftID)	Configuring RADIUS Authentication
Cisco Duo Security Authentication Manager Server	• Token-based authentication	Integration of SMA with Cisco Duo Security MFA Server
One Identity Defender	• Username/password • Token-based authentication (such as SecurID or SoftID)	One Identity Defender
RSA Authentication Manager Server	• Token-based authentication (such as SecurID or SoftID)	Configuring RSA Server Authentication
Public key infrastructure (PKI)	• Digital certificate (with optional certificate revocation checking)	Configuring a PKI Authentication Server
SAML 2.0 Identity Provider	• Username/password	Configuring a SAML-Based Authentication Server
Local users (local user storage)	• Username/password	Configuring Local User Storage

For further information about tasks after configuring the authentication server, see:

- Defining Multiple Authentication Servers
- Disabling Authorization Checks

- Configuring Chained Authentication
- Enabling Group Affinity Checking in a Realm
- Using One-Time Passwords for Added Security

Defining Multiple Authentication Servers

The SMA appliance supports the definition and use of multiple authentication servers. A community determines which access agents are provisioned to your users and what End Point Control restrictions (if any) are imposed. See Users, Groups, Communities, and Realms for more about community.

Following are examples of using multiple authentication servers referenced by realms:

- **Chained authentication (two authentication servers)**

  Example: RADIUS with Token/SecurID and LDAP with username/password

  Users logging in to a realm are authenticated against two servers. You can configure AMC so that users see only one prompt. See Configuring Chained Authentication for details.

- **Use different servers to handle authentication and authorization**

  Example: RADIUS with Token/SecurID and Active Directory (for group information)

  The user authenticates against one repository, and then the user’s group information is passed from a second one. For more information, see Enabling Group Affinity Checking in a Realm.

- **Multiple credential types and a single authentication server**

  Example: RADIUS with username/password and RADIUS with Token/SecurID

  Suppose your company employees log in with username and password, but the employees of your call-center log in with SecurID tokens. You could create an *employee* realm and a *callcenter* realm, each referencing the appropriate credential type and RADIUS server.

- **Multiple instances of the same directory/authentication method using different back-end servers**

  Example: Two RADIUS/password instances using different RADIUS servers

  In this case you would define two authentication servers, each with the appropriate server information.

- **Multiple instances of the same directory/authentication method on the same server, configured differently**

  Example: Two instances of LDAP with username/password on the same server but using different search bases

  In this case each realm would search a different subtree within the directory. For example, suppose Partner A is in one LDAP subtree and Partner B is in another. You could define a partnerA realm and a partnerB realm, each configured with the appropriate search base.

Disabling Authorization Checks

You can optionally disable the querying of group information used for authorization when configuring an authentication server. A **Use this authentication server to check group membership** checkbox is available for each server type that can contain group information used for authorization, including Active Directory, Active Directory Tree, and LDAP servers.

Usually, when you use a directory server as part of authentication, you also want the group information stored there to be used in policy authorization. However, in some cases a directory server is used for secondary authentication and does not contain group information. In other cases, the secondary authentication server does not use the same identifier for the user.

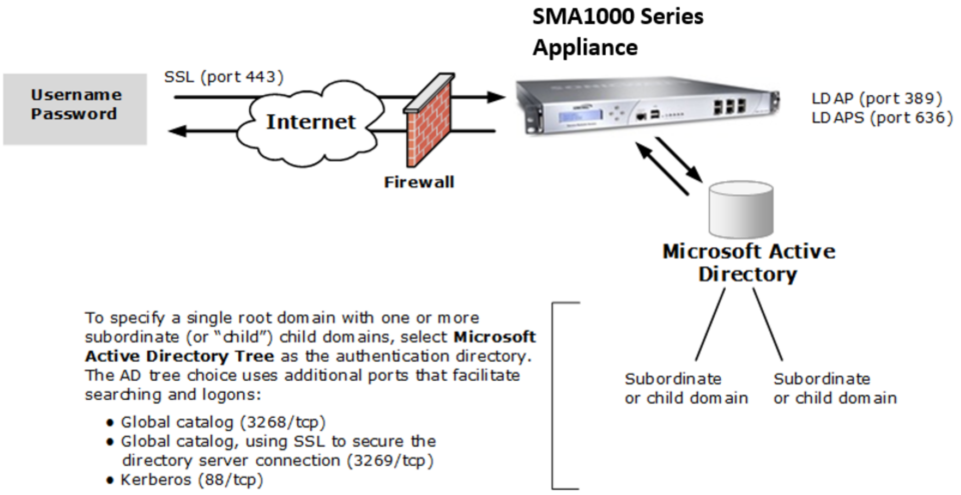
If a group query is made on both a primary and a secondary server, the authentication process takes longer. However, if the user name is different on the two servers, a group query using the name from the primary server will result in an error from the secondary server. Since the appliance policy always defaults to closed, such an error will result in any deny rule being applied to the end user. By disabling group authorization checks on the secondary server, you can avoid these problems.

If group checking is disabled for an authentication server, the server will not be available in the list of available affinity servers on the realm configuration page. Conversely, if an authentication server is in use as an affinity server for any realm, group checking cannot be disabled for that authentication server. See Enabling Group Affinity Checking in a Realm for more information.

Configuring Microsoft Active Directory Servers

The appliance can validate username/password credentials against Microsoft Active Directory (AD) configured with either a single root domain, or one or more subordinate (child) domains. The below image shows typical Active Directory configuration options.

Microsoft Active Directory Configuration Options



To specify a single root domain with one or more subordinate (or "child") child domains, select **Microsoft Active Directory Tree** as the authentication directory. The AD tree choice uses additional ports that facilitate searching and logons:

- Global catalog (3268/tcp)
- Global catalog, using SSL to secure the directory server connection (3269/tcp)
- Kerberos (88/tcp)

You must modify your firewall or router to allow the appliance to communicate with your AD server. The appliance uses standard LDAP and LDAPS ports to communicate with Active Directory:

- LDAP (389/tcp)
- LDAP over SSL (636/tcp)

With Microsoft Active Directory Advanced there are additional ports, which facilitate searches and logons:

- Global catalog (3268/tcp)
- Global catalog using SSL (3269/tcp)
- Kerberos (88/tcp)

After configuring an AD server, you can validate the realm configuration settings by establishing a test connection. For more information, see Testing AD,LDAP,RADIUS and One Defender Authentication Configurations.

Topics:

- Configuring Active Directory with Username and Password
- Configuring Multiple Active Directory (Advanced)
- Configuring LDAP to Authenticate Against Active Directory
- LDAP Examples for Active Directory Authentication

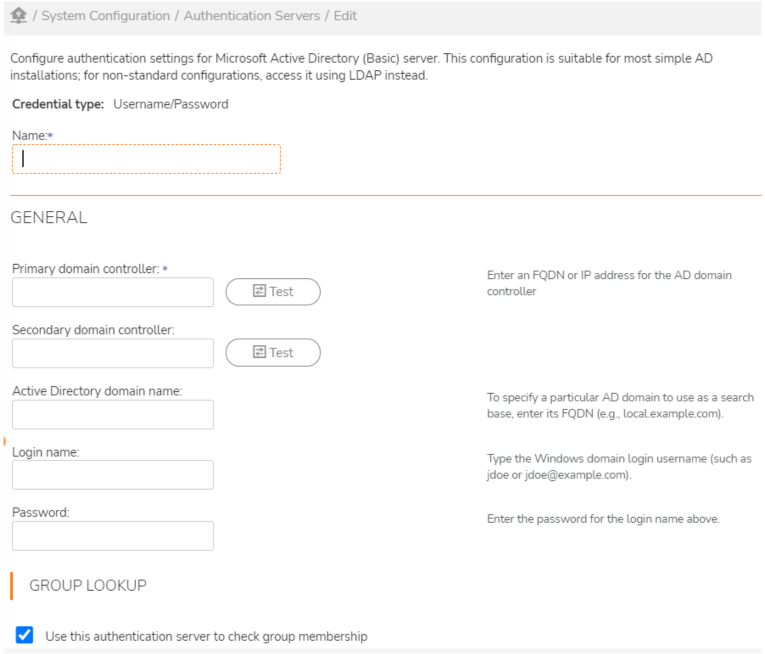
Configuring Active Directory with Username and Password

ⓘ | **NOTE:**

- If you are using Active Directory with digital certificates, you must configure AD as an LDAP realm. See Configuring LDAP to Authenticate Against Active Directory.
- If your AD authentication server has subordinate (child) domains, see Configuring Multiple Active Directory (Advanced) for more information.

To configure an Active Directory authentication server with username/password validation:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New** and select **Microsoft Active Directory (Basic)**.



/ System Configuration / Authentication Servers / Edit

Configure authentication settings for Microsoft Active Directory (Basic) server. This configuration is suitable for most simple AD installations; for non-standard configurations, access it using LDAP instead.

Credential type: Username/Password

Name:*

GENERAL

Primary domain controller: * Test — Enter an FQDN or IP address for the AD domain controller

Secondary domain controller: Test

Active Directory domain name: — To specify a particular AD domain to use as a search base, enter its FQDN (e.g., local.example.com).

Login name: — Type the Windows domain login username (such as jdoe or jdoe@example.com).

Password: — Enter the password for the login name above.

GROUP LOOKUP

☑ Use this authentication server to check group membership

3. In the **Name** field, type a name for the authentication server.
4. In the **Primary domain controller** field, type the IP address or host name of the AD domain controller. If you are using a failover server (optional), specify its address in the **Secondary domain controller** field.

   If the AD server is listening on a something other than the well-known port (389 for unencrypted connections, or 636 for SSL connections), specify a port number as a colon-delimited suffix (for example, `ad.example.com:1300`).
5. To specify a particular AD domain, type it in the **Active Directory domain name** field. This should be the domain that you want to use as the search base (in other words, the domain that contains the appropriate `cn=users` container). For example, if you want to search a single domain such as *marketing*, type `marketing.example.com`. If you want to search your entire company's domain, type `example.com`. If you do not specify a domain, the appliance searches the first available default naming context on the domain controller.
6. To perform AD searches, the appliance must log in to Active Directory (unless you have configured AD to allow anonymous searches). In the **Login name** field, type the username or **sAMAccountname** attribute used to log in to the Windows domain (such as `jdoe` or `jdoe@example.com`).

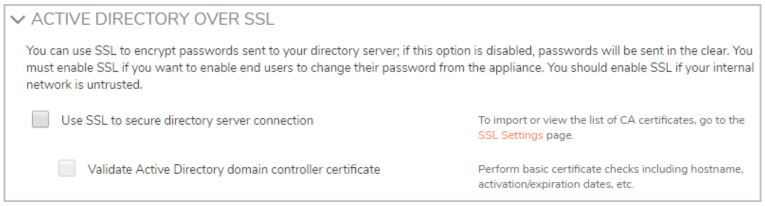
   The login should be for a user who has privileges to perform searches and view user records, such as the administrator on that domain controller. You may also specify a non-administrator user who has these privileges.

   If you specify an AD domain, the appliance searches that domain for users. If you do not specify a domain, the appliance searches the first available default naming context on the domain controller. If the user information is not stored in either of these locations, you need to configure this realm as an LDAP realm. See Configuring LDAP to Authenticate Against Active Directory.
7. Type the **Password** that corresponds to the **Login name**. After you've entered credentials, you can click the **Test** button for each server you specified in order to test the connection.

8. Complete the information listed under **Group lookup**:

   - To enable group checking on this server, select the **Use this authentication server to check group membership** checkbox. When this box is unchecked, the nested controls are disabled because they apply only to group checking behavior. This checkbox, when unselected, allows an authentication server for LDAP, AD, or AD-Tree to be configured without enabling it for authorization checks. This improves efficiency by allowing better stacked/affinity authentication support.
   - To specify the depth of the search (how many sub-groups to include in it), enter a number in the **Nested group lookup** checkbox. Be aware that this type of search can take some time because it requires searching the entire Active Directory tree; enabling **Cache group checking** is highly recommended.
   - To reduce the load on your directory and get better performance, cache the attribute group or static group search results. Select the Cache group checking checkbox and then specify a **Cache lifetime**, in seconds. The default value is *1800* seconds (30 minutes).

9. To secure the AD connection with SSL, expand the **Active Directory over SSL** area, and the configure the following settings:



ACTIVE DIRECTORY OVER SSL

You can use SSL to encrypt passwords sent to your directory server; if this option is disabled, passwords will be sent in the clear. You must enable SSL if you want to enable end users to change their password from the appliance. You should enable SSL if your internal network is untrusted.

□ Use SSL to secure directory server connection — To import or view the list of CA certificates, go to the SSL Settings page.

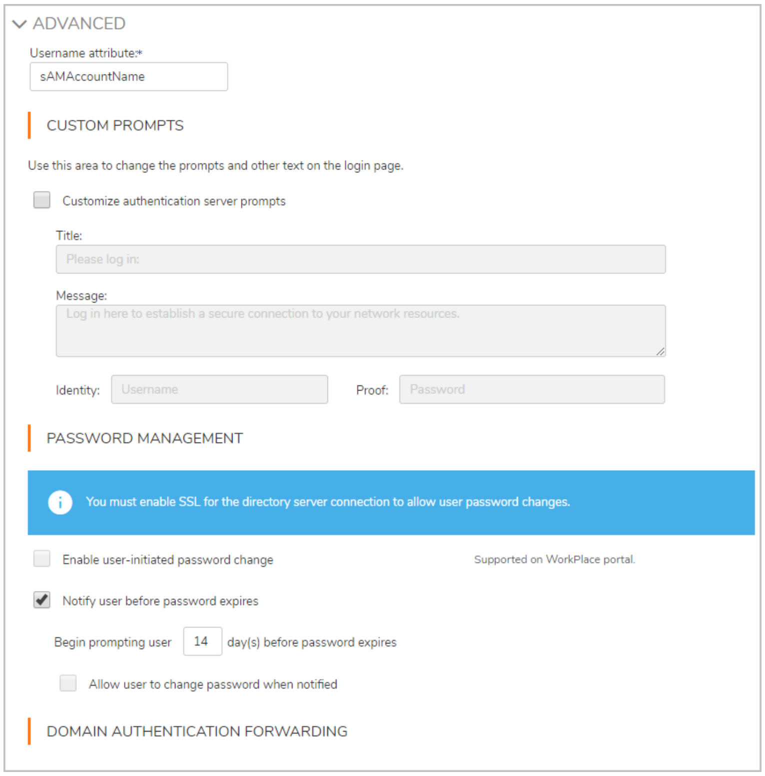
□ Validate Active Directory domain controller certificate — Perform basic certificate checks including hostname, activation/expiration dates, etc.

   a. Select the **Use SSL to secure directory server connection** checkbox.

   b. To view your certificate details and to verify that the root certificate can be used by the appliance, click the **SSL Settings** link. This list should show the name of the CA (or CAs) that issued the client certificates and the SSL certificates. If your AD server's CA is not listed in the file, or if you use a self-signed certificate, you must add your certificate to this file. See Importing CA Certificates for details.

   c. To have the appliance verify that the AD domain controller host name is the same as the name in the certificate presented by the Active Directory server, select the **Match Active Directory domain controller certificate** checkbox. Typically, your server name will match the name specified in its digital certificate. If this is the case with your server, SonicWall recommends enabling this option in a production environment. This makes it more difficult for an unauthorized server to masquerade as your AD server if your digital certificate or DNS server is compromised.

10. In the **Advanced** area, you can specify a username attribute, set up custom prompts, enable users to be notified of expiring Active Directory passwords, configure NTLM authentication forwarding options, and set up one-time passwords.



ADVANCED

Username attribute:* sAMAccountName

CUSTOM PROMPTS

Use this area to change the prompts and other text on the login page.

□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username Proof: Password

PASSWORD MANAGEMENT

You must enable SSL for the directory server connection to allow user password changes.

□ Enable user-initiated password change Supported on WorkPlace portal.

☑ Notify user before password expires

Begin prompting user 14 day(s) before password expires

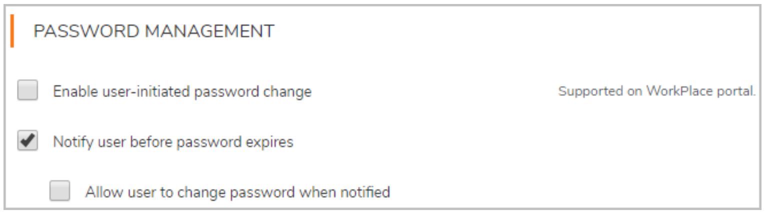
□ Allow user to change password when notified

DOMAIN AUTHENTICATION FORWARDING

11. Type the **Username attribute** you want to use to match user names. In most AD implementations, **sAMAccountName** matches the user ID (for example, *jdoe*). You can use `cn` instead, but that would require the user to authenticate with his full name (*John Doe*) instead of his user ID (*jdoe*).

12. To change the prompts and other text that Windows users see when they log in to the authentication server, select the **Customize authentication server prompts** checkbox. If users should log in using an employee ID, for example, you could change the text for the **Identity** prompt from **Username**: to **Employee ID**. (If you plan to use chained authentication, customized password prompts are especially useful so that users can differentiate between them.)

13. If the connection between the appliance and the authentication server is secured with SSL (**Use SSL to secure Active Directory connection** is enabled), you can allow users to change their passwords in WorkPlace by selecting **Enable user-initiated password change**.



PASSWORD MANAGEMENT

□ Enable user-initiated password change Supported on WorkPlace portal.

☑ Notify user before password expires

□ Allow user to change password when notified

CAUTION: If Active Directory over SSL is not enabled, passwords are transmitted in the clear to the AD server. If the internal network is not trusted, you should enable SSL. Your AD server must also be enabled to use SSL. See the Microsoft AD documentation for details.

NOTE:

- The **Login name** and **Password** fields are not always required to connect to an Active Directory server. However, if they are not provided (or you don't specify a password) the appliance will bind anonymously. In this case, if you have not configured Active Directory to allow anonymous searches, the search will fail.
- Users must have permission on the AD server to change their passwords during the password notification period, and the administrator must have permission to change user passwords after they expire. For security reasons, both of these operations replace passwords rather than reset them.
- If you define multiple Active Directory with SSL servers, you should specify the same **Match certificate CN against Active Directory domain controller** setting for each server. (SonicWall recommends enabling this option for a production environment.) Although AMC allows you to configure this setting on a per-realm basis, the appliance actually uses the setting specified in the last loaded ADS realm. For example, if you select this checkbox for three ADS realms, but clear it for a fourth, the functionality would be disabled for all four realms.

14. To allow the Active Directory server to notify users that their passwords are going to expire, select the **Notify user before password expires** checkbox. Indicate when the advance notice should begin (the default is **14** days, and the maximum is 30 days). The password prompt users see is controlled by the AD server.
15. To allow users to manage their own passwords, select the **Allow user to change password when notified** checkbox. This setting can be changed only if the **Use SSL to secure Active Directory connection** checkbox in the **Active Directory over SSL** area is selected. Password management is available only to users with Web access and those who are using Connect Tunnel.
16. To enable NTLM authentication forwarding, click one of the **NTLM authentication forwarding** options. For more information, see NTLM Authentication Forwarding.
17. To configure authentication that includes an OTP, enable **Use one-time passwords with this authentication server**.

    a. To send OTP through Email/SMTP, you must configure the SMTP service. For more details, see Configuring SMTP to Deliver One-Time Passwords.

    - Enter the number of characters for the OTP in the **Password contains** field. The default length is 6, the minimum is 4, and the maximum is 20.
    - • Select the type of characters in the OTP from the drop-down menu. Select **Alphabetic and numeric**, or **Numeric**.
    - In the **From address** field, enter the email address from which the OTP will be sent.
    - In the **Primary email address attribute** field, enter the directory attribute for the email address to which one-time passwords will be sent. If the primary attribute exists on the authentication server, it is used.
    - The **Secondary email address attribute**, if specified, is used in addition to the primary email address. The OTP is sent to both addresses.

      To have OTPs sent as a text message (instead of an email message), enter the corresponding attribute name (for example, `SMSphone` instead of `Mail` or `primaryEmail`). See Configuring the AD or LDAP Directory Server for more information.

- In the **Subject** field, customize the subject line of the OTP email. You can use the replacement variable *{password}* to indicate a position in the subject line where the actual password will display.
- In the **Body** field, customize the body of the OTP message. Use the replacement variable *{username}* to indicate a position in the message where the user's account name will display. Use the replacement variable *{password}* to indicate a position in the message where the actual password will display.
- To test delivery of an OTP to a user, enter the email address of the user who will receive the OTP into the **Email address** field and click the **Send test message** button. If the appliance is able to send the message, the status `Message successfully sent` is displayed below the button. Failure messages are also displayed below the button, such as errors connecting to the SMTP server, or errors communicating with the AD/LDAP server or looking up the specified user on the AD/LDAP server.

ⓘ **NOTE:** You can configure OTP to be delivered through SMS and Email or only through SMS or only through Email. Same OTP will be delivered through both the channels.

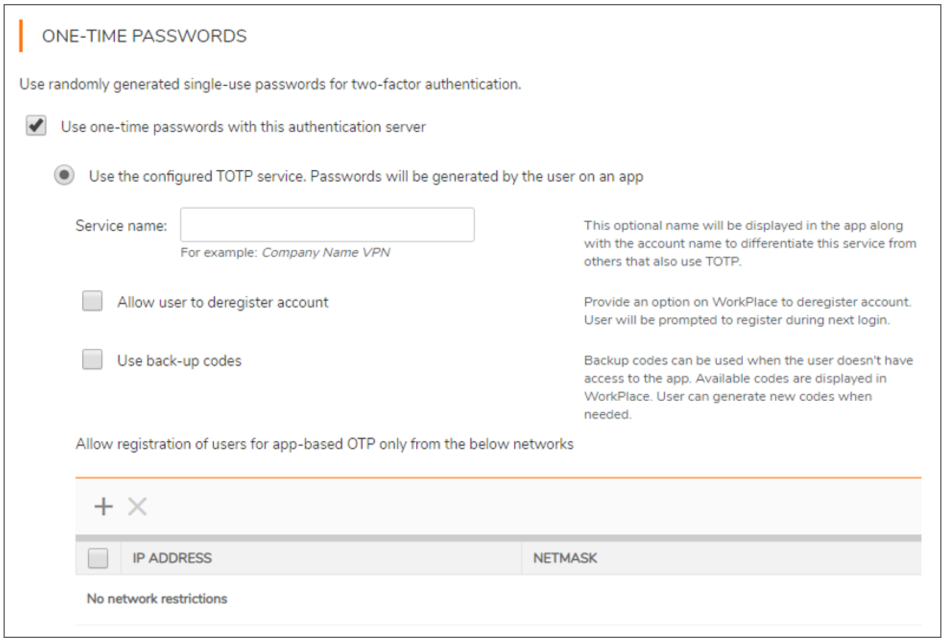
b. To send OTP through SMS, you must configure the SMS service. For more details, see Configuring an Authentication Server for email-basedOne-Time Passwords

- Enable **Send password via text message using SMS** option.
- Enter the number of characters for the OTP in the **Password** field. The default length is 6, the minimum is 4, and the maximum is 20.
- Select the type of characters in the OTP from the drop-down menu. Select **Alphabetic**, **Alphabetic and numeric**, or **Numeric**.
- Choose masking level of user phone number shown on authentication page after sending OTP. This helps the user to know to which number the OTP is being sent.
  - Choose **Partial** if only part of phone number should be displayed.
  - Choose **None** if whole phone number should be displayed.
  - Choose **Full** if no phone number should be displayed.
- In the **Phone number attribute** field, enter the directory attribute for the phone number to which one-time passwords will be sent.
- In the **Message** field, customize the body of the OTP message. Use the replacement variable {username} to indicate a position in the message where the user's account name will display. Use the replacement variable {password} to indicate a position in the message where the actual password will display.
- To test delivery of an OTP to a user, enter the phone number of the user who will receive the OTP into the **Phone number** field and click the **Send test message** button. If the appliance is able to send the message, the status Message successfully sent is displayed below the button. Failure messages are also displayed below the button, such as errors connecting to the SMS gateway server.
- To use **Time based OTP**, you must enable "Use the configured TOTP service" under Authentication servers. For more details, see Configuring Time-Based One-Time Passwords Settings.

ⓘ **NOTE:** When you are upgrading from prior versions of SMA to 12.4, TOTP service and the configuration information is automatically moved from global configuration to authentication server.

- Select **Use the configured TOTP service** option. Password will be generated by the user on their application.
- In the **Service name** field, you can configure an individual name for authentication servers. This optional name will be displayed in the application along with the account name to differentiate the service from others that also use TOTP.
- If you want the user to deregister account, enable **Allow user to deregister account**. This will provide an option on CT and Workplace for user to deregister their account.
- Backup codes can be used when the user does not have access to their application. Available codes are displayed in CT and WorkPlace. User can generate new codes when needed only once in 24 hours. To provide back up code option to users, enable **Use back-up codes**.
- You can configure list of networks where you can restrict registration of users from unauthenticated networks. Click + icon to configure the trusted networks that should be used by the users for the application based TOTP registration.
- Export/Import of TOTP configuration containing registered user data is supported (on full import).

ⓘ **NOTE:** If you have not configured any trusted networks, TOTP account registration is allowed from any network.



ONE-TIME PASSWORDS

Use randomly generated single-use passwords for two-factor authentication.

☑ Use one-time passwords with this authentication server

● Use the configured TOTP service. Passwords will be generated by the user on an app

Service name:
For example: *Company Name VPN*

This optional name will be displayed in the app along with the account name to differentiate this service from others that also use TOTP.

□ Allow user to deregister account

Provide an option on WorkPlace to deregister account. User will be prompted to register during next login.

□ Use back-up codes

Backup codes can be used when the user doesn't have access to the app. Available codes are displayed in WorkPlace. User can generate new codes when needed.

Allow registration of users for app-based OTP only from the below networks

□	IP ADDRESS	NETMASK
	No network restrictions	

18. Click **Save**.

Configuring Multiple Active Directory (Advanced)

This feature expands user authentication and authorization from one Active Directory (AD) advanced to multiple AD trees within a trusted forest and AD Federated Forests. Configuring AD multi-forest/multi-realm support consists of the following steps:

1. Configure AD forest authentication server with AD domains from the current AD forest and trusted forests enabled.
2. Configure groups.

Once AD multi-forest/multi-realm support is configured, users from the designated forests can be authenticated and log into WorkPlace and Connect Tunnel.

ⓘ | **NOTE:** A trusted domain is a domain that authenticates users when they login.

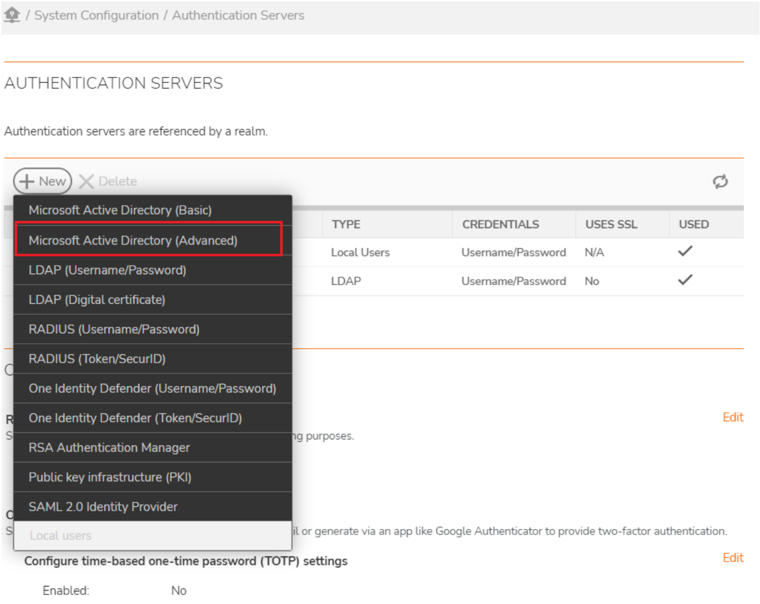
Topics:

- Configure AD Forest Authentication Server
- Configure Groups Using Multiple Trees
- Configure Groups Using Trees from Trusted Forests
- User Login

Configure AD Forest Authentication Server

Configure the AD forest authentication server and enable AD domains from the current AD forest and trusted forests:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New** in the **Authentication servers** section.
3. Select **Microsoft Active Directory (Advanced)**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

TYPE	CREDENTIALS	USES SSL	USED
Local Users	Username/Password	N/A	✓
LDAP	Username/Password	No	✓

ng purposes.

il or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings

Enabled: No

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
Edit
Edit

4. Select any other applicable options and click **Continue** to advance to the **Configure Authentication Server** page.

5. In the **Name** field, type the name that will be used to identify the Active Directory tree or forest.
6. In the **Root Domain** field, type the AD root domain of the forest.
7. Check the **Enable cross-forest trust** checkbox to enable appliance access to other trusted forests. If not enabled, the appliance can access only the forest in a direct trust relationship with the configured forest.
8. In the **Login name** and **Password** fields, type the user name and password for a user who has read access to the entire Forest.

Configure Groups Using Multiple Trees

Create groups of users and groups imported from the AD domains in the forest. Only users and groups from the configured forest are included when cross-forest trust is disabled.

Configure Groups Using Trees from Trusted Forests

Create groups of users and groups imported from AD Domains in the configured forest and trusted forests. Users and groups from the configured forest and all trusted forests are included when cross-forest trust is enabled.

User Login

Once AD multi-forest/multi-realm support is configured, users from the designated forests can be authenticated and log into WorkPlace and Connect Tunnel.

Users login to WorkPlace or Connect Tunnel using one of the following:

- Username in UPN form (for example, `joe.user@company.com`) and password
- Username, Password and Domain - when Domain Selection option is configured)
- Username and Password – when a default domain is configured

Configuring LDAP to Authenticate Against Active Directory

If you have customized Active Directory (by, for example, specifying a search base instead of using the AD default), you need to authenticate to Active Directory using LDAP. The procedure for configuring an LDAP server is defined in Configuring LDAP and LDAPS Authentication. When configuring LDAP, you should pay special attention to the attributes you're using to query the directory. Because every implementation of AD is different, you must know how the object classes and related attributes are configured in your Active Directory schema.

ⓘ **NOTE:** When an Active Directory (AD) server is used as an LDAP server, ACL checks cannot be performed. on Short names (SN) or common names (CN) are not supported on LDAP servers. They are only supported on AD servers.

The following table describes the key AD attributes used to validate username and password credentials. The attributes are not case-sensitive.

AD Attributes For Credential Validation

Field	Description

Login DN	The DN used to establish a connection with your Active Directory server. In a generic AD configuration located in the *`example.com`* domain, the DN for a user named John Doe would be: `cn=John Doe,cn=users,dc=example,dc=com`
Search base	The point in the AD directory from which you want to search for user information. Usually, this is the lowest point in the directory tree that contains user information. The user binding to AD must have permissions to view the directory at this level. For a generic installation, a search base of `cn=users,dc=example,dc=com` will find most users. You may want to search from a higher level (such as `dc=example,dc=com`) if some users are stored in a different branch.
Username attribute	The attribute used to match usernames. In most AD implementations, **sAMAccountName** matches the user ID (for example, *jdoe*). You can use `cn` instead, but that would require the user to authenticate with his full name (*John Doe*) instead of his user ID (*jdoe*).

If you create an access control rule that references a group, a user must be an explicit member of that group forhis or her request to match the rule. To include nested groups when evaluating group membership, make sure that **Nested group lookup** is set accordingly when you configure the authentication server in AMC.

For example, assume that the *SeattleCampus* group contains a group called *Marketing*. Employee *John Doe* is a member of the *Marketing* group, but is not explicitly a member of *SeattleCampus*. If **Nested group lookup** is set to *0*, the appliance will not recognize *John Doe* as a member of the *SeattleCampus* group; if it is set to *1*, he is recognized.

Microsoft provides a graphical tool that makes it easy to perform LDAP operations, including connecting, browsing, and modifying a directory. The tool—called LDP (`ldp.exe`)—is available with the Support Tools for the Windows Server platform; see the Microsoft Product Support site for more information.

LDAP Examples for Active Directory Authentication

Example 1—Active Directory

Active Directory Configuration 1

Login DN	*CN=AVtest,CN=Users,DC=testusrs,DC=example,DC=com*
Search base	*DC=testusrs,DC=example,DC=com*
Username attribute	*sAMAccountName*

Example 2—Active Directory

Active Directory Configuration 2

Login DN	*CN=johnDoe,CN=Users,DC=na,DC=example,DC=com*
Search base	*CN=Users,DC=na,DC=example,DC=com*
Username attribute	*sAMAccountname*

Example 3—LDAP with Domino Server

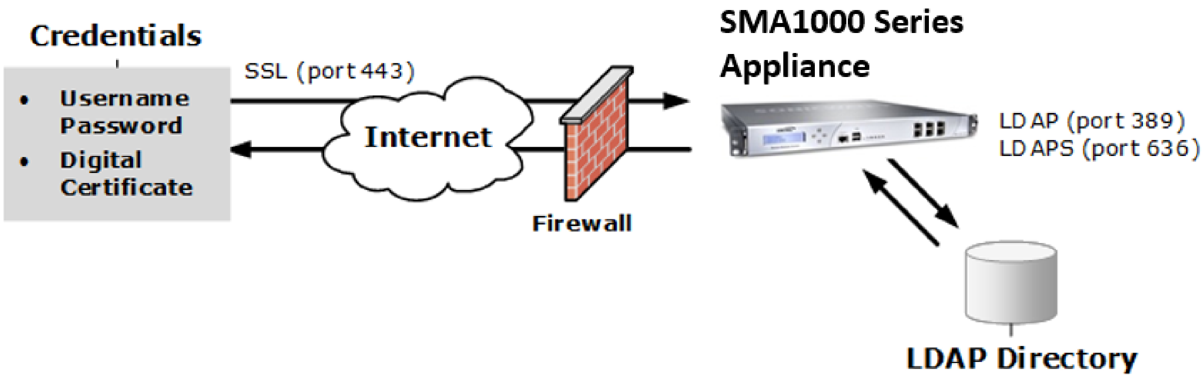
LDAP Configuration With Domino Server

Login DN	*CN=E-Class SMA,O=peoplesoft*
Search base	*o=peoplesoft*
Username attribute	*cn*

Configuring LDAP and LDAPS Authentication

The SMA appliance supports authentication using the LDAP or LDAPS (LDAP over SSL) protocols. Either protocol can be used to validate username and password credentials. The below image shows typical LDAP configuration options.

LDAP And LDAPS Authentication Configuration Options



Securing your LDAP connection with SSL requires additional configuration. You must add the root certificate of the CA that granted your LDAP certificate to the SSL trusted CA certificates. This enhances security by preventing attempts to impersonate your LDAP server. For more information, see Importing CA Certificates.

After configuring an LDAP or LDAPS server, you can validate the realm configuration settings by establishing a test connection. For more information, see Testing AD,LDAP,RADIUS and One Defender Authentication Configurations.

Consider the following restrictions when configuring LDAP authentication:

- **Firewalls and routers** - You must configure your firewall or router to allow the appliance to communicate with your LDAP server. Standard LDAP uses port 389/tcp; LDAPS communicates over port 636/tcp.

- **LDAP Affinity servers** - Although it is possible to configure LDAP Affinity servers for all authentication servers, an Affinity server should be used only for an authentication server that does not include full group search capabilities, such as a RADIUS, RSA, and PKI server. In addition, Secure Mobile Access does not support Affinity servers for stacked authentication where any one of the authentication servers has group checking capabilities.

  ⓘ **NOTE:** When an Active Directory (AD) server is used as an LDAP server, ACL checks cannot be performed on. Short names (SN) or common names (CN) are not supported on LDAP servers. They are only supported on AD servers.

- **Digital certificate validation** - Configuring an LDAP authentication server with digital certificate validation is offered for legacy customers. New users should use the standard method described in Configuring a PKI Authentication Server. The **Trust intermediate CAs without verifying the entire chain** option is offered on the configuration pages for both the **LDAP** with **Digital Certificate** option and the **Public key infrastructure** (PKI) option.

Topics:

- Configuring LDAP with Username and Password
- Configuring a PKI Authentication Server
- Importing CA Certificates
- About Intermediate Certificates

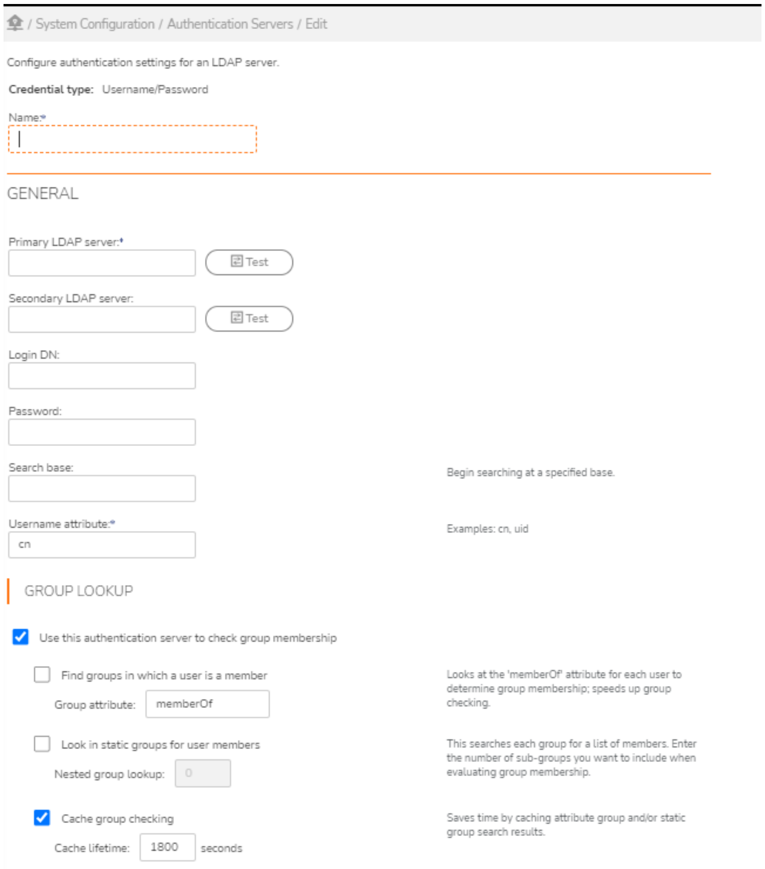
Configuring LDAP with Username and Password

Remember the following when configuring LDAP:

- The **Notify user before password expires** and **Allow user to change password when notified**settings in the **Password management** area have some constraints:
  - They are supported only on IBM Directory Server.
  - They are available only for users who connect to the appliance using Web access (the translated, custom port mapped, or custom FQDN mapped Web access), or using Connect Tunnel.
  - Users must have permission on the LDAP server to change their passwords.
- The **Login DN** and **Password** fields are not always required in order to connect to an LDAP server. However, if they are not provided (or you do not specify a password), the appliance binds to LDAP anonymously, which does not usually provide the appropriate permissions for performing user and group information searches.

To configure an LDAP authentication server with username and password validation:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.
3. Under **Authentication directory**, click **LDAP**.



/ System Configuration / Authentication Servers / Edit

Configure authentication settings for an LDAP server.

Credential type: Username/Password

Name:*

GENERAL

Primary LDAP server:* Test

Secondary LDAP server: Test

Login DN:

Password:

Search base: — Begin searching at a specified base.

Username attribute:* cn — Examples: cn, uid

GROUP LOOKUP

☑ Use this authentication server to check group membership

☐ Find groups in which a user is a member — Looks at the 'memberOf' attribute for each user to determine group membership; speeds up group checking.

Group attribute: memberOf

☐ Look in static groups for user members — This searches each group for a list of members. Enter the number of sub-groups you want to include when evaluating group membership.

Nested group lookup: 0

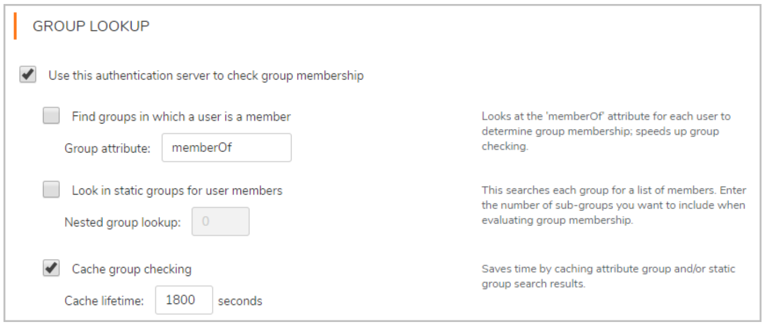
☑ Cache group checking — Saves time by caching attribute group and/or static group search results.

Cache lifetime: 1800 seconds

4. In the **Name** field, type a name for the authentication server.
5. Complete the information listed under **General:**
   - In the **Primary LDAP server** field, type the host name or IP address of your LDAP server. If you are using a failover server (optional), specify its address in the **Secondary LDAP server** field.

     If the LDAP server is listening on a something other than the well-known port (389 for unencrypted LDAP connections, or 636 for SSL connections), specify a port number as a colon-delimited suffix (for example, `myldap.example.com:1300`).
   - In the **Login DN** field, type the distinguished name (DN) used to establish a connection with the LDAP server.
   - In the **Password** field, type the password used to establish a connection with the LDAP server.
   - In the **Search base** field, type the point in the LDAP directory from which you want to begin searching for user information. This will usually be the lowest point in the directory advanced that contains user information. For example, you might type `ou=Users,o=xyz.com`. The user binding to the LDAP directory must have permissions to view the directory at this level.
   - In the **Username attribute** field, type the attribute used to match usernames. This is usually `cn` or `uid`.
   - Click the **Test** button for each server you specified in order to test the connection.

6. Complete the information listed under **Group lookup**:



GROUP LOOKUP

☑ Use this authentication server to check group membership

□ Find groups in which a user is a member

Group attribute: memberOf

Looks at the 'memberOf' attribute for each user to determine group membership; speeds up group checking.

□ Look in static groups for user members

Nested group lookup: 0

This searches each group for a list of members. Enter the number of sub-groups you want to include when evaluating group membership.

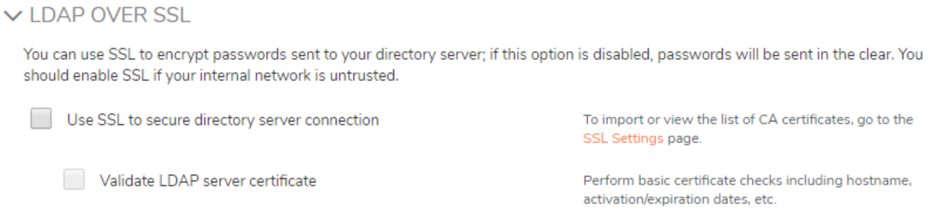
☑ Cache group checking

Cache lifetime: 1800 seconds

Saves time by caching attribute group and/or static group search results.

- To enable group checking on this server, select the **Use this authentication server to check group membership** checkbox. When this checkbox is unchecked, the nested controls are disabled because they apply only to group checking behavior. This checkbox, when unselected, allows an authentication server for LDAP, AD, or AD-Advanced to be configured without enabling it for authorization checks. This improves efficiency by allowing better stacked/affinity authentication support.
- If you want the LDAP search to determine a user's group membership by searching the group attribute in the user container, select the **Find groups in which a user is a member** checkbox and then type the **Group attribute**. This attribute is most often **memberOf**. Do not select this checkbox unless attribute-based groups are supported by and enabled on your LDAP server.
- If your LDAP server does not support attribute-based groups or you have not enabled this functionality, you can select the **Look in static groups for user members** checkbox; to specify the depth of the search (how many sub-groups to include in the search), enter a number in the **Nested group lookup** checkbox. Be aware that this type of search can take some time because it requires searching the entire LDAP advanced; enabling **Cache group checking** is highly recommended.
- To reduce the load on your directory and get better performance, cache the attribute group or static group search results. Select the **Cache group checking** checkbox and then specify a **Cache lifetime**, in seconds. The default value is **1800** seconds (30 minutes).

7. To secure the LDAP connection with SSL, complete the information under **LDAP over SSL**:



LDAP OVER SSL

You can use SSL to encrypt passwords sent to your directory server; if this option is disabled, passwords will be sent in the clear. You should enable SSL if your internal network is untrusted.

□ Use SSL to secure directory server connection

To import or view the list of CA certificates, go to the SSL Settings page.

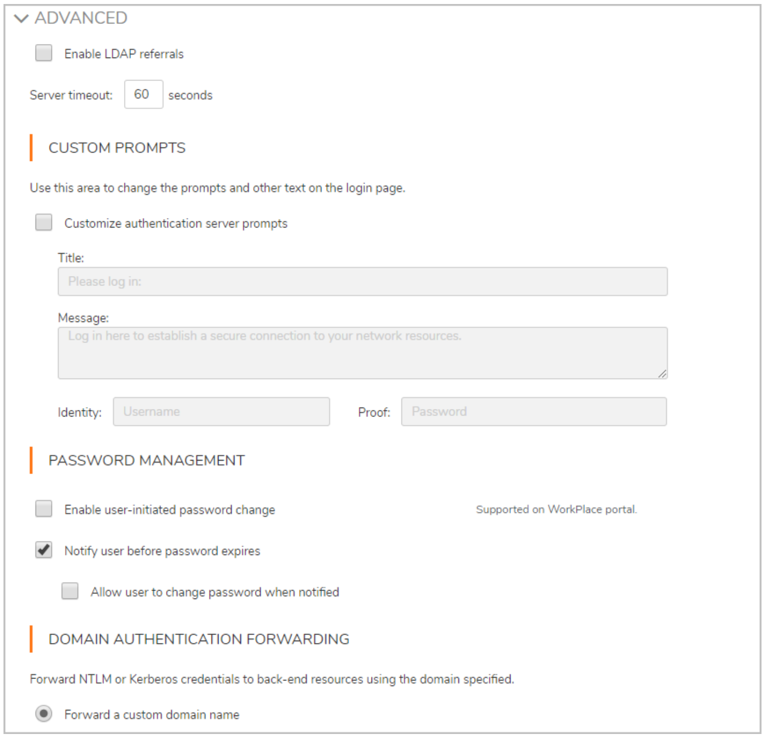
□ Validate LDAP server certificate

Perform basic certificate checks including hostname, activation/expiration dates, etc.

- To secure the LDAP connection with SSL, select the **Use SSL to secure LDAP connection** checkbox.
- View your certificate details and verify that the root certificate can be used by the appliance. See Importing CA Certificates for details.

- To configure the appliance to verify that the LDAP host name is the same as the name in the certificate presented by the LDAP server, select the **Match certificate CN against LDAP server name** checkbox. Typically, your server name will match the name specified in its digital certificate. If this is the case with your server, SonicWall recommends enabling this option in a production environment. This makes it more difficult for an unauthorized server to masquerade as your LDAP server if your digital certificate or DNS server is compromised.

8. Optionally, complete the information listed under **Advanced**.



ADVANCED

□ Enable LDAP referrals

Server timeout: 60 seconds

CUSTOM PROMPTS

Use this area to change the prompts and other text on the login page.

□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username   Proof: Password

PASSWORD MANAGEMENT

□ Enable user-initiated password change   Supported on WorkPlace portal.

☑ Notify user before password expires

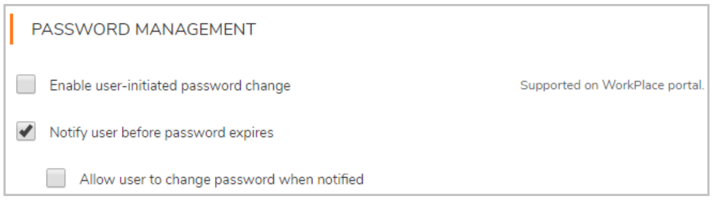
□ Allow user to change password when notified

DOMAIN AUTHENTICATION FORWARDING

Forward NTLM or Kerberos credentials to back-end resources using the domain specified.

● Forward a custom domain name

- When an LDAP server cannot answer a client's query, you can refer it to other LDAP servers by selecting the **Enable LDAP referrals** checkbox. Use caution when enabling this feature because it can slow down the authentication process. If you are configuring LDAP to authenticate against Microsoft Active Directory, you may want to disable this feature.
- In the **Server timeout** field, type the number of seconds to wait for a reply from the LDAP server. The default value is **60** (one minute).
- To change the prompts and other text that Windows users see when they log in to the authentication server, select the **Customize authentication server prompts** checkbox. The page title, message, and login prompts can all be customized. If users log in using a PIN as a password, for example, change the text for the **Proof** prompt from **Password:** to **PIN:** (a customized **Message** could explain how to retrieve a forgotten PIN).
- You can allow users to change their passwords (in WorkPlace only) by selecting **Enable user-initiated password change**. If a realm is configured with stacked authentication and requires two sets of username/password credentials, a user who changes his or her password will be changing the credentials for just the first of the two authentication servers.



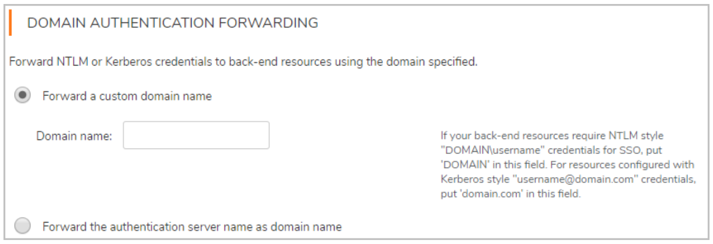
PASSWORD MANAGEMENT

☐ Enable user-initiated password change — Supported on WorkPlace portal.

☑ Notify user before password expires

☐ Allow user to change password when notified

- To allow the LDAP server to notify users that their passwords are going to expire, select the **Notify user before password expires** checkbox. To also permit them to change their passwords when prompted by the LDAP server, select the **Allow user to change password when notified** checkbox. The password prompt users see is controlled by the LDAP server.
- To enable NTLM authentication forwarding, click one of the **Domain authentication forwarding** options. For more information, see NTLM Authentication Forwarding.



DOMAIN AUTHENTICATION FORWARDING

Forward NTLM or Kerberos credentials to back-end resources using the domain specified.

● Forward a custom domain name

Domain name:

If your back-end resources require NTLM style "DOMAIN\username" credentials for SSO, put 'DOMAIN' in this field. For resources configured with Kerberos style "username@domain.com" credentials, put 'domain.com' in this field.

○ Forward the authentication server name as domain name

9. To configure authentication that includes an OTP, enable **Use one-time passwords with this authentication server**.

   a. To send OTP through Email/SMTP, you must configure the SMTP service. For more details, see Configuring SMTP to Deliver One-Time Passwords.

   - Enter the number of characters for the OTP in the **Password contains** field. The default length is 6, the minimum is 4, and the maximum is 20.
   - Select the type of characters in the OTP from the drop-down list. Select **Alphabetic**, **Alphabetic and numeric**, or **Numeric**.
   - In the **From address** field, enter the email address from which the OTP will be sent.
   - In the **Primary email address attribute** box, enter the directory attribute for the email address to which one-time passwords will be sent. If the primary attribute exists on the authentication server, it is used.
   - The **Secondary email address attribute**, if specified, is used in addition to the primary email address. The OTP is sent to both addresses.

     To have OTPs sent as a text message (instead of an email message), enter the corresponding attribute name (for example, `SMSphone` instead of `Mail` or `primaryEmail`). See Configuring the AD or LDAP Directory Server for more information.
   - In the **Subject** field, customize the subject line of the OTP email. You can use the replacement variable *{***password***}* to indicate a position in the subject line where the actual password will display.
   - In the **Body** field, customize the body of the OTP message. Use the replacement variable *{***username***}* to indicate a position in the message where the user's account name will display. Use

the replacement variable *{password}* to indicate a position in the message where the actual password will display.

- To test delivery of an OTP to a user, enter the email address of the user who will receive the OTP into the **Email address** field and click the **Send test message** button. If the appliance is able to send the message, the status `Message successfully sent` is displayed below the button. Failure messages are also displayed below the button, such as errors connecting to the SMTP server, or errors communicating with the AD/LDAP server or looking up the specified user on the AD/LDAP server.

ⓘ **NOTE:** You can configure OTP to be delivered through SMS and Email or only through SMS or only through Email. Same OTP will be delivered through both the channels.

b. To send OTP through SMS, you must configure the SMS service. For more details, see Configuring an Authentication Server for email-basedOne-Time Passwords

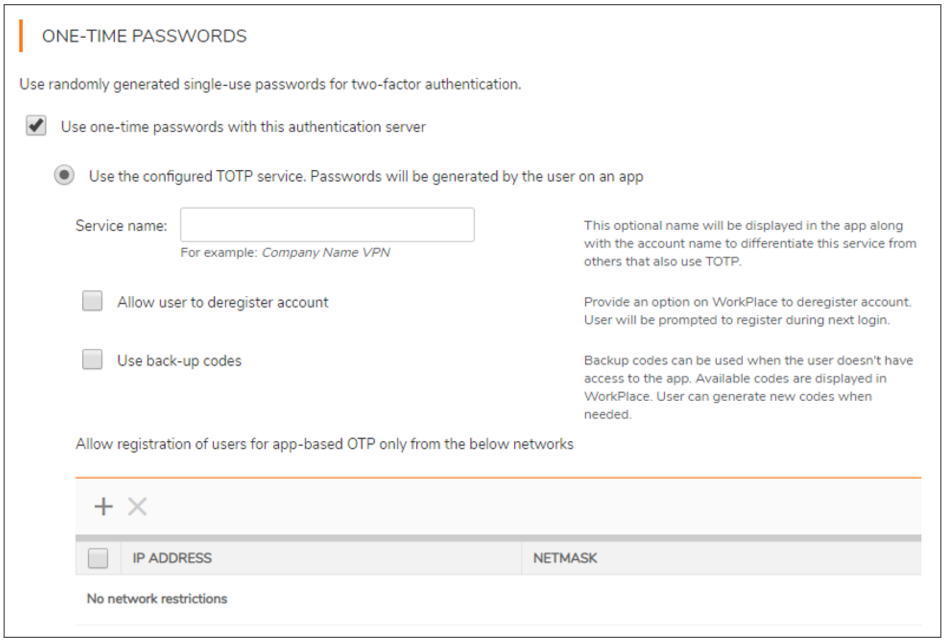
- Enable **Send password via text message using SMS** option.
- Enter the number of characters for the OTP in the **Password** field. The default length is 6, the minimum is 4, and the maximum is 20.
- Select the type of characters in the OTP from the drop-down menu. Select **Alphabetic**, **Alphabetic and numeric**, or **Numeric**.
- Choose masking level of user phone number shown on authentication page after sending OTP. This helps the user to know to which number the OTP is being sent.
    - Choose **Partial** if only part of phone number should be displayed.
    - Choose **None** if whole phone number should be displayed.
    - Choose **Full** if no phone number should be displayed.
- In the **Phone number attribute** field, enter the directory attribute for the phone number to which one-time passwords will be sent.
- In the **Message** field, customize the body of the OTP message. Use the replacement variable {username} to indicate a position in the message where the user's account name will display. Use the replacement variable {password} to indicate a position in the message where the actual password will display.
- To test delivery of an OTP to a user, enter the phone number of the user who will receive the OTP into the **Phone number** field and click the **Send test message** button. If the appliance is able to send the message, the status Message successfully sent is displayed below the button. Failure messages are also displayed below the button, such as errors connecting to the SMS gateway server.
- To use **Time based OTP**, you must enable "Use the configured TOTP service" under Authentication servers. For more details, see Configuring Time-Based One-Time Passwords Settings.

ⓘ **NOTE:** When you are upgrading from prior versions of SMA to 12.4, TOTP service and the configuration information is automatically moved from global configuration to authentication server.

- Select **Use the configured TOTP service** option. Password will be generated by the user on their application.

- In the **Service name** field, you can configure an individual name for authentication servers. This optional name will be displayed in the application along with the account name to differentiate the service from others that also use TOTP.
- If you want the user to deregister account, enable **Allow user to deregister account**. This will provide an option on workplace for user to deregister their account.
- Backup codes can be used when the user does not have access to their application. Available codes are displayed in WorkPlace. User can generate new codes when needed only once in 24 hours. To provide back up code option to users, enable **Use back-up codes**.
- You can configure list of networks where you can restrict registration of users from unauthenticated networks. Click + icon to configure the trusted networks that should be used by the users for the application based TOTP registration.

ⓘ **NOTE:** If you have not configured any trusted networks, TOTP account registration is allowed from any network.


ONE-TIME PASSWORDS

Use randomly generated single-use passwords for two-factor authentication.

☑ Use one-time passwords with this authentication server

● Use the configured TOTP service. Passwords will be generated by the user on an app

Service name: For example: *Company Name VPN*

This optional name will be displayed in the app along with the account name to differentiate this service from others that also use TOTP.

☐ Allow user to deregister account

Provide an option on WorkPlace to deregister account. User will be prompted to register during next login.

☐ Use back-up codes

Backup codes can be used when the user doesn't have access to the app. Available codes are displayed in WorkPlace. User can generate new codes when needed.

Allow registration of users for app-based OTP only from the below networks

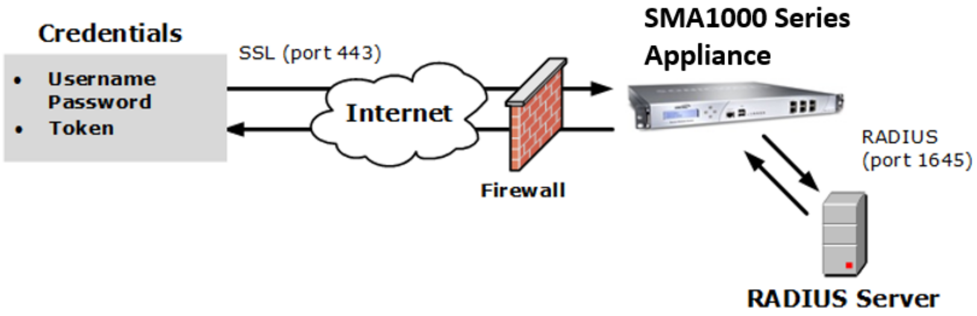
☐	IP ADDRESS	NETMASK
	No network restrictions	

10. Click **Save**.

Configuring RADIUS Authentication

The appliance can validate username/password or token-based credentials against a RADIUS database. The below image shows typical RADIUS configuration options:

RADIUS Authentication Configuration Options



You must modify your firewall or router to allow the appliance to communicate with your RADIUS server. The RADIUS authentication protocol typically uses port 1645/udp. In addition, you must configure your RADIUS server to include the IP address of the appliance as a RADIUS client (most often referred to as a *Network Access Server*).

ⓘ **NOTE:** Affinity servers should be used only for authentication servers that do not include full group search capabilities, such as RADIUS, RSA, and PKI servers.

Topics:

- Configuring RADIUS with User or Token-Based Credentials
- Configuring Advanced RADIUS Settings

Configuring RADIUS with User or Token-Based Credentials

The appliance supports two different types of credentials for RADIUS: username and password, and token-based user credentials, such as SecurID or SoftID, which are validated against a database on a RADIUS server. You can configure the RADIUS authentication method to use either type of credential.

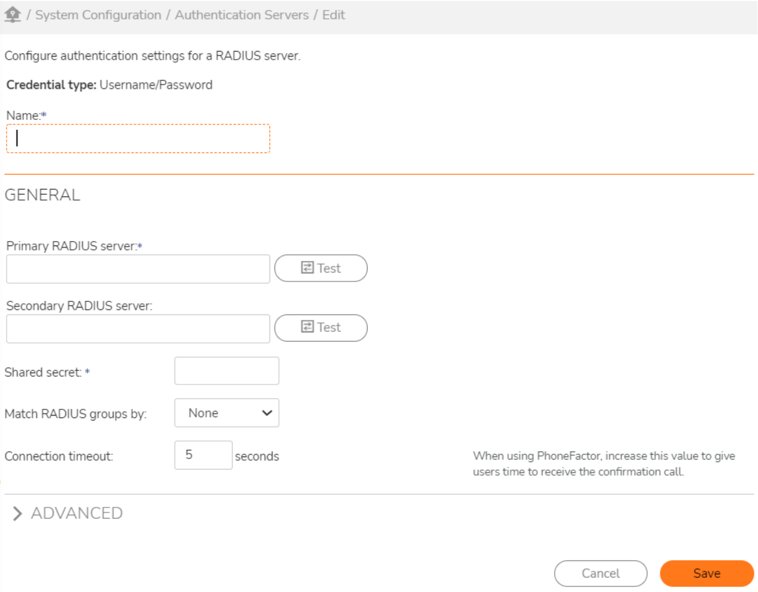
You can also deploy PhoneFactor authentication using RADIUS. When a user logs into their company's VPN, a RADIUS request is made to the PhoneFactor Agent, which acts as a RADIUS proxy server. It first validates the user name and password with the target RADIUS server before initiating a PhoneFactor authentication. There are two methods for two-factor authentication using PhoneFactor:

- The user enters his username and password and is then called by PhoneFactor. The user answers his phone and presses # or enters a PIN.
- The user enters his username and password and then PhoneFactor sends him a text message containing a one-time passcode. The user replies to the text message with the passcode, or the passcode and his PIN, to authenticate.

To configure RADIUS for user- or token-based credentials:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.

3. Click **RADIUS**.



/ System Configuration / Authentication Servers / Edit

Configure authentication settings for a RADIUS server.

Credential type: Username/Password

Name:*

GENERAL

Primary RADIUS server:*

Secondary RADIUS server:

Shared secret: *

Match RADIUS groups by: None

Connection timeout: 5 seconds

When using PhoneFactor, increase this value to give users time to receive the confirmation call.

4. In the **Name** field, type a name for the authentication server.
5. In the **Primary RADIUS server** field, type the host name or IP address of your primary RADIUS server. If your RADIUS server is listening on a port other than 1645 (the well-known port for RADIUS), you can specify a port number as a colon-delimited suffix (`:<port number>`).
6. In the **Secondary RADIUS server** field, type the host name or IP address of your secondary RADIUS server. You can also add a port number if necessary.
7. In the **Shared secret** field, type the password used to secure communication with the RADIUS server. This must be the same secret that is specified on the designated RADIUS server.
8. In the **Match RADIUS groups by** list, select the attribute containing the groups of which the user is a member. The value returned from RADIUS will be used in the group portion of the appliance access rule. There are three possible values:

RADIUS Groups Matching

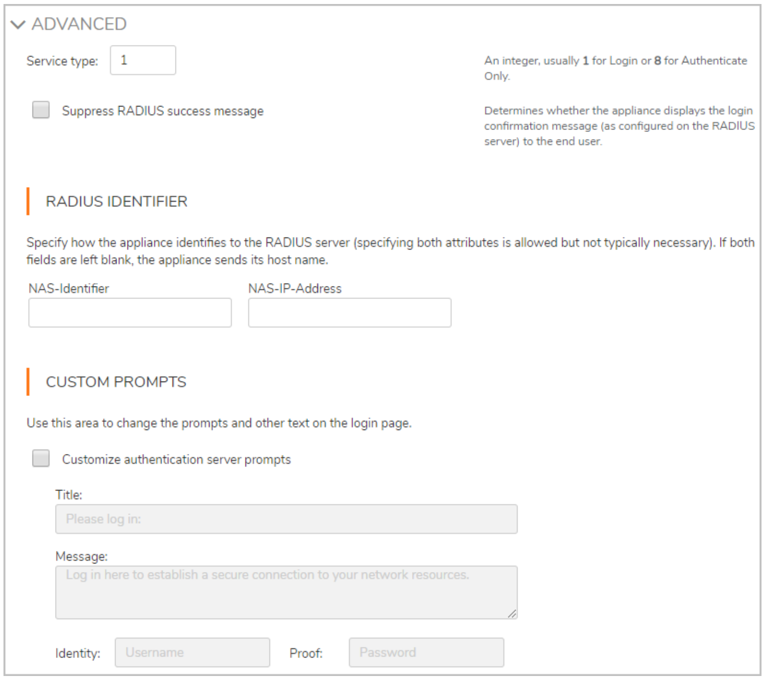
Match RADIUS groups by	Description
None	Ignores the group attribute
filterid attribute (11)	Matches against the **FilterID** attribute
class attribute (25)	Matches against the **Class** attribute

9. In the **Connection timeout** field, type the number of seconds to wait for a reply from the RADIUS server before timing out the authentication attempt. The default is 5 seconds, with a range of 5 to 300 seconds. When using PhoneFactor, increase this value to give users time to receive the confirmation call.
10. Expand the **Advanced** button to see additional, optional settings; these are described in Configuring Advanced RADIUS Settings.
11. Click **Save**.

Configuring Advanced RADIUS Settings

To configure additional (optional) RADIUS settings:

1. Click the **Advanced** button to display additional (optional) RADIUS settings.



ADVANCED

Service type: 1

An integer, usually **1** for Login or **8** for Authenticate Only.

□ Suppress RADIUS success message

Determines whether the appliance displays the login confirmation message (as configured on the RADIUS server) to the end user.

RADIUS IDENTIFIER

Specify how the appliance identifies to the RADIUS server (specifying both attributes is allowed but not typically necessary). If both fields are left blank, the appliance sends its host name.

NAS-Identifier

NAS-IP-Address

CUSTOM PROMPTS

Use this area to change the prompts and other text on the login page.

□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username Proof: Password

2. In the **Service type** field, type a RADIUS Service-Type integer indicating the type of service being requested. For most RADIUS servers, type **1** (for Login; default) or **8** (for Authenticate Only).

3. When a user’s credentials are accepted, the RADIUS server normally sends a confirmation message (for example, `Passcode accepted`). If you do not want this message displayed, select the **Suppress RADIUS success message** checkbox.

4. Select the authentication protocol method from the drop-down. The supported authentication protocol methods include PAP, CHAP, MSCHAP, and MSCHAPv2.

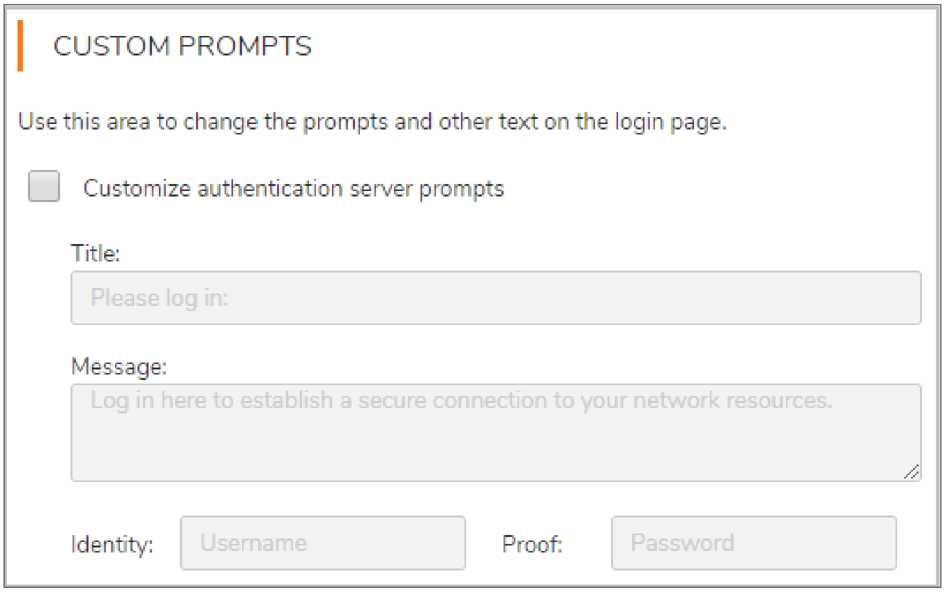
   > **NOTE:** If you have selected the authentication protocol method as MSCHAPv2, **Allow password changes** check box is enabled. Selecting this checkbox allows users to change the password when the password gets expired or when the password is reset by the administrator.

   > **NOTE:** In order to support CHAP authentication protocol method, user passwords must be stored using reversible encryption in the Operating System. In **Windows Security policy security setting & AD users properties > Account** tab, enable “Store passwords using reversible encryption”.

5. The appliance normally identifies itself using its host name. If the RADIUS server is unable to accept that name, specify a **NAS-Identifier** or **NAS-IP-Address** (specifying both is allowed but not typically necessary).

6. To change the prompts and other text that Windows users see when they log in to the authentication server, select **Customize authentication server prompts**. The page title, message, and login prompts

can all be customized. For example, if a user logs in using his employee ID, you could change the text for the **Identity**prompt from **Username**: to **Employee ID**:



CUSTOM PROMPTS

Use this area to change the prompts and other text on the login page.

□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username Proof: Password

7. If the RADIUS server uses an older version of the RADIUS protocol that does not support UTF-8 character encoding, select a **Local encoding** scheme from the **Selected** list, or type one in the **Other** field. For more information, see RADIUS Policy Server Character Sets.

8. (RADIUS with a **Credential type** of **Username/Password** only) To enable NTLM authentication forwarding, click one of the **NTLM authentication forwarding** options. For more information, see NTLM Authentication Forwarding.

Integration of SMA with Cisco Duo Security MFA Server

The SMA1000 appliance can be integrated with Cisco Duo Security Multiple Factor Authentication (MFA) server. This allows users to choose a second factor authentication method on SMA clients to prove their identity. Upon providing primary credentials, users are provided with a list of devices and authentication methods registered with Duo for the user. User can choose an authentication method to authenticate. Based on user choice, user needs to either respond to Push notification or phone-call or other OTP methods and proceed with authentication. Users who fail to authenticate against Cisco Duo Security MFA server will be denied login access.

This authentication server can be attached to any primary authentication server supported by SMA. This authentication server automatically uses the username provided for primary authentication, thus the user does not have to enter username again for Cisco Duo Security MFA authentication.

As an admin you can check if the user's IP is forwarded to Cisco Duo Security MFA server, so that Cisco Duo Security can enforce network related policy enforcement.

Prerequisites:

- SMA/CMS running 12.4.3 firmware version.
- Ensure you have an active license or partnership with Cisco Duo Security service to do MFA.

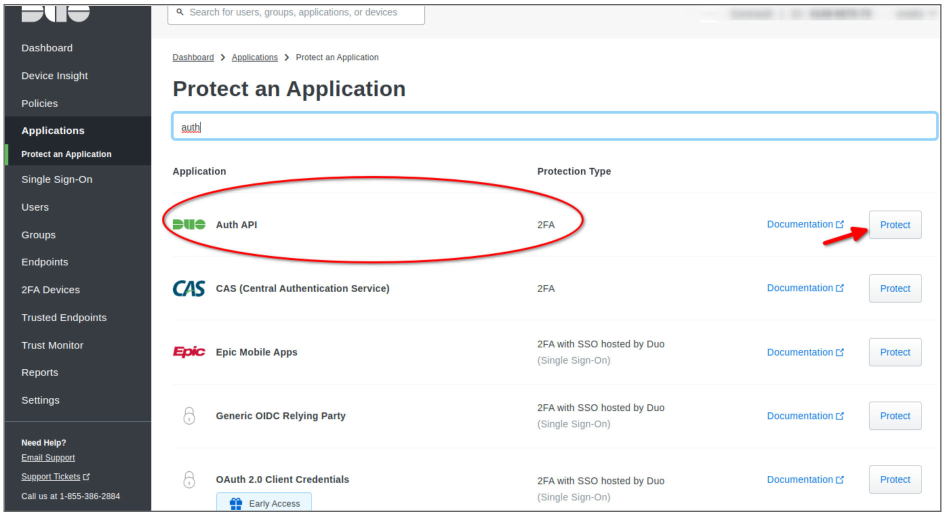
Topics:

- Configuring Cisco Duo security MFA server
- Configuring Cisco Duo Security MFA Server in SMA1000
- Enrolling users for Cisco Duo Security MFA Server
- Additional Authentication Methods
- SMA1000 Clients and AMC authentication support

Configuring Cisco Duo security MFA server

To configure Cisco Duo Security MFA Server, do the following:

1. Log in to the Duo Admin Panel.
2. In Duo Admin Panel, select **Applications** > **Protect an Application**.
3. Search Auth API in the applications list and click **Protect**.

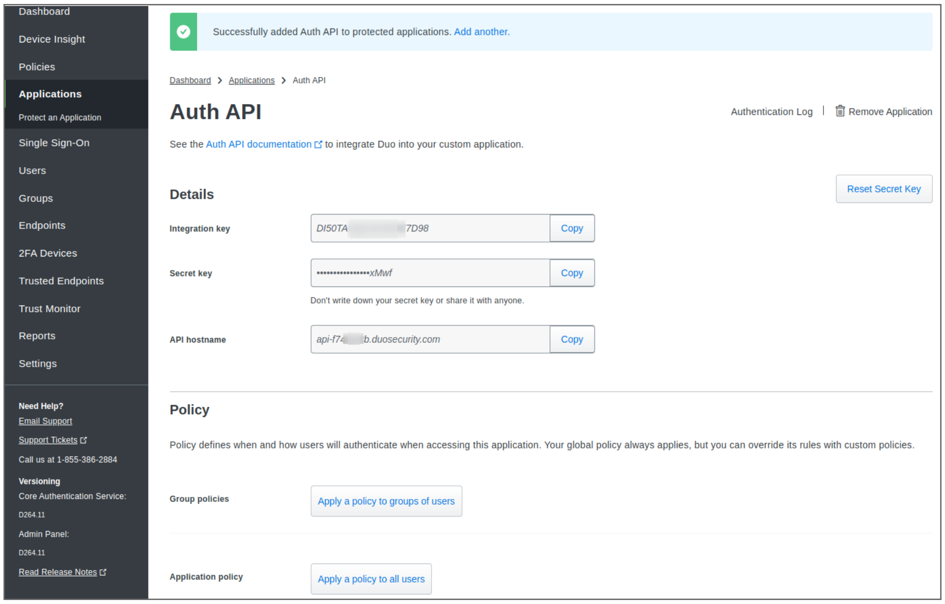


Protect an Application

auth

Application	Protection Type		
Auth API	2FA	Documentation	Protect
CAS (Central Authentication Service)	2FA	Documentation	Protect
Epic Mobile Apps	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
Generic OIDC Relying Party	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
OAuth 2.0 Client Credentials Early Access	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

The application generates an **Integration key**, **Secret key**, and **API hostname.** Copy this information to configure on SMA1000.



Successfully added Auth API to protected applications. Add another.

Auth API

See the Auth API documentation to integrate Duo into your custom application.

Details

Integration key	DI50TA[redacted]7D98
Secret key	••••••••••••••••xMwf Don't write down your secret key or share it with anyone.
API hostname	api-f74[redacted]b.duosecurity.com

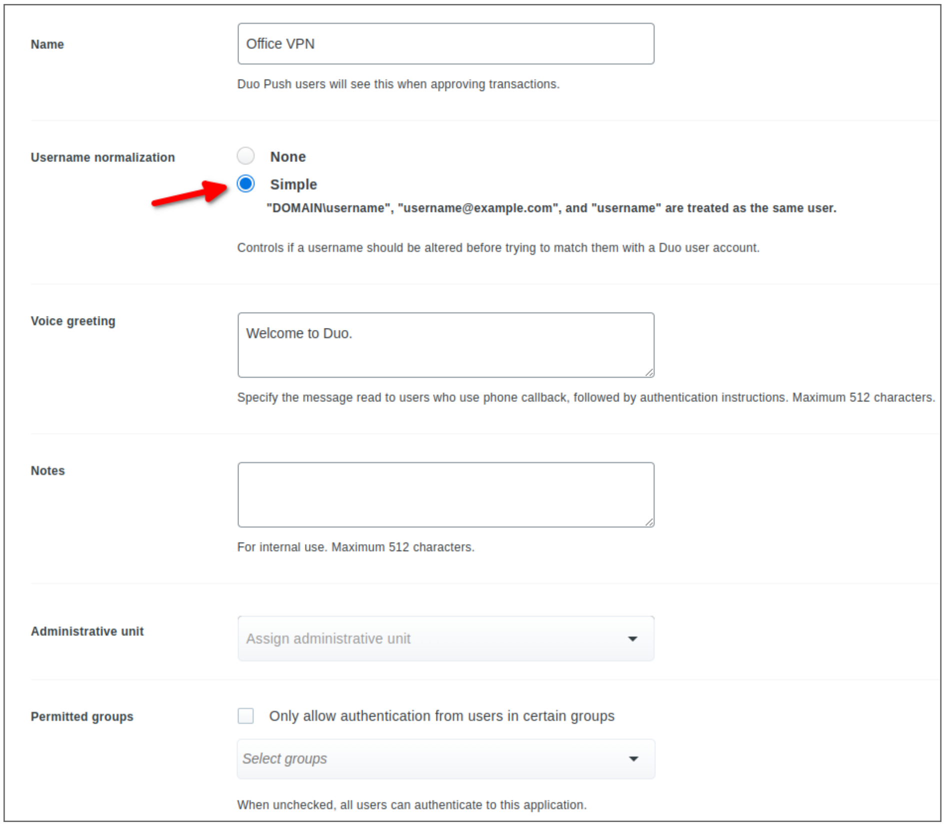
Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Application policy

4. Choose **Username normalization** as **Simple**.



Name	Office VPN Duo Push users will see this when approving transactions.
Username normalization	○ None ● Simple "DOMAIN\username", "username@example.com", and "username" are treated as the same user. Controls if a username should be altered before trying to match them with a Duo user account.
Voice greeting	Welcome to Duo. Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.
Notes	For internal use. Maximum 512 characters.
Administrative unit	Assign administrative unit
Permitted groups	□ Only allow authentication from users in certain groups *Select groups* When unchecked, all users can authenticate to this application.

5. Review policy and other settings.

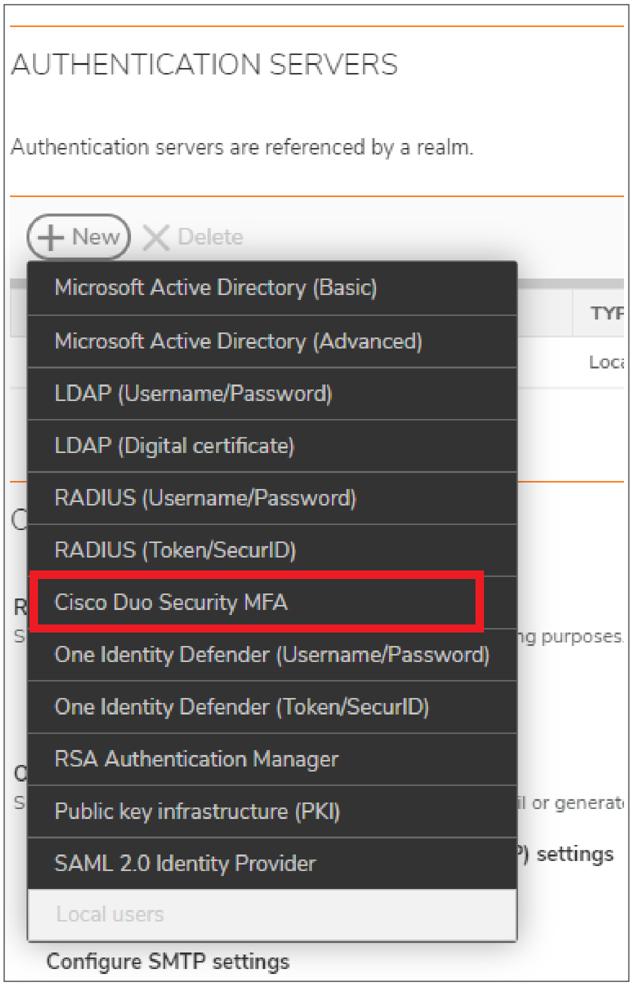
6. Click **Save**.
7. Go to SMA1000 AMC and configure authentication settings for Cisco Duo Security MFA server. See Configuring Cisco Duo Security MFA Server in SMA1000.

Configuring Cisco Duo Security MFA Server in SMA1000

Configure authentication settings for Cisco Duo Security Multi-Factor Authentication server in SMA1000 AMC.

To configure, do the following:

1. In AMC, navigate to **System Configuration** > **Authentication Servers**.
2. Click **New** and select **Cisco Duo Security MFA**.



AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

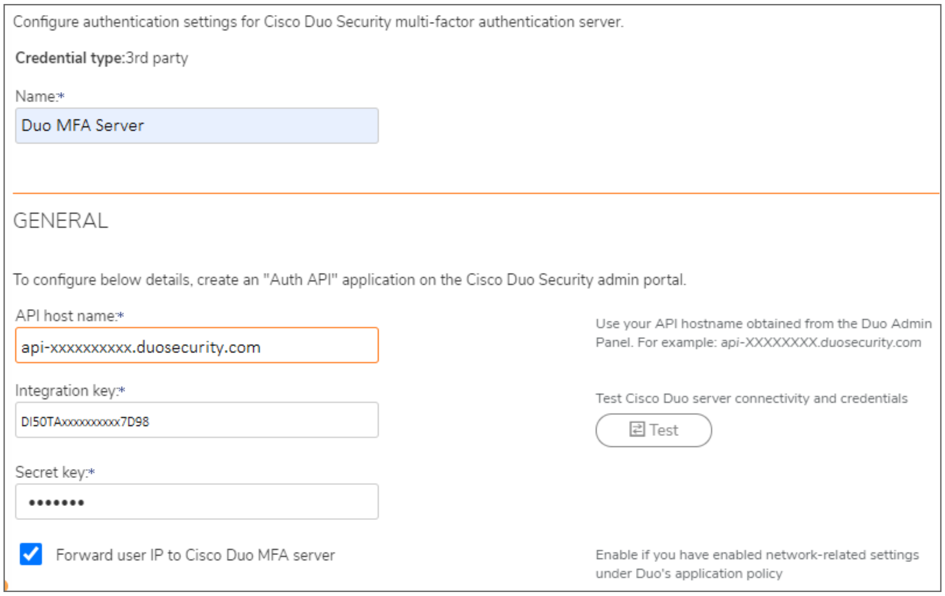
+ New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
Configure SMTP settings

3. In the **Name** field, type a name for the authentication server.
4. Under the **General** section, enter the following keys copied from Duo admin portal:

a. **API hostname** is a valid FQDN.

b. **Integration key**, should be of minimum 1 character and maximum of 100 characters length.

c. **Secret key**, should be of minimum 1 character and maximum of 100 characters length.



Configure authentication settings for Cisco Duo Security multi-factor authentication server.

Credential type:3rd party

Name:* Duo MFA Server

GENERAL

To configure below details, create an "Auth API" application on the Cisco Duo Security admin portal.

API host name:* api-xxxxxxxxxx.duosecurity.com

Use your API hostname obtained from the Duo Admin Panel. For example: api-XXXXXXXX.duosecurity.com

Integration key:* DI50TAxxxxxxxxxxx7D98

Test Cisco Duo server connectivity and credentials

Secret key:* •••••••

☑ Forward user IP to Cisco Duo MFA server

Enable if you have enabled network-related settings under Duo's application policy

5. Enable **Forward user IP to Cisco Duo MFA** if you have enabled network-related settings under Duo's application policy server. By default this **Forward user IP to Cisco Duo MFA** check box is enabled. See Networks Policy Settings.

6. Click **Test** to test appliance connectivity with Duo MFA server and verify credentials.

7. Next enroll users for Cisco Duo Security Multi-Factor Authentication. See Enrolling users for Cisco Duo Security MFA Server.

.

Enrolling users for Cisco Duo Security MFA Server

SMA1000 allows users enroll with Cisco Duo Security Multi-Factor Authentication.

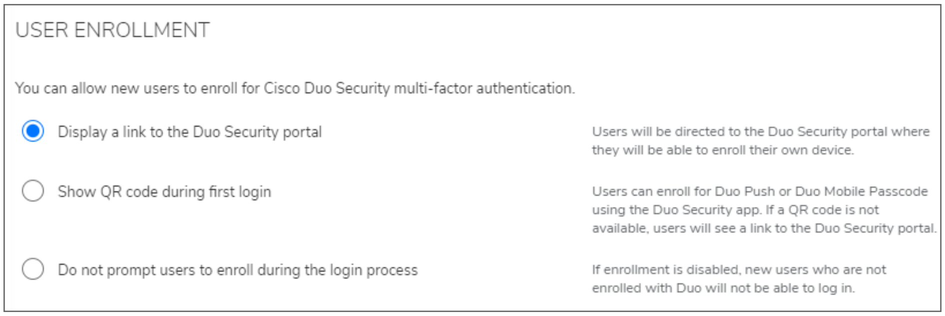
This procedure is only for the users who are not added to Cisco Duo Security MFA server on admin portal or for users who are added at the server but no devices attached. For the users who already have a device (phone or token), irrespective of whether they are in-possession or lost, will not see the enrollment option. In case if a phone is lost, the user must reach the admin to remove the lost device and so that the user can see the enroll option during next login.

To configure new user enrollment with Cisco Duo Security MFA, do the following:

1. In the AMC, navigate to **System Configuration** > **Authentication Servers** > **Cisco Duo Security MFA**.

   ⓘ **NOTE:** Duo MFA authentication fails if appliance clock is incorrect. Synchronize with NTP server to avoid Duo MFA authentication failures.

2. Under the **User Enrollment** section, choose the following enrollment methods for the users:



USER ENROLLMENT

You can allow new users to enroll for Cisco Duo Security multi-factor authentication.

● Display a link to the Duo Security portal — Users will be directed to the Duo Security portal where they will be able to enroll their own device.

○ Show QR code during first login — Users can enroll for Duo Push or Duo Mobile Passcode using the Duo Security app. If a QR code is not available, users will see a link to the Duo Security portal.

○ Do not prompt users to enroll during the login process — If enrollment is disabled, new users who are not enrolled with Duo will not be able to log in.

Enrollment method	Description
Display a link to the Duo Security portal	• User can enroll their mobile phone number to avail Push notification, mobile code, Phone call, text message and other OTP methods. • After enrollment, user can continue with Duo MFA authentication. This option is enabled by default.
Show QR code during first login	• New users are shown a QR code that can be scanned using Duo mobile app. This associates the mobile with user account. • User can enroll for push and mobile code authentication methods. • After enrollment, user can continue with Duo MFA authentication.
Do not prompt users to enroll during the login process	Users who are not enrolled with Cisco Security Duo MFA server will not be able to log in to SMA.

3. Select additional authentication methods for users to enroll the devices. See Additional Authentication Methods

Additional Authentication Methods

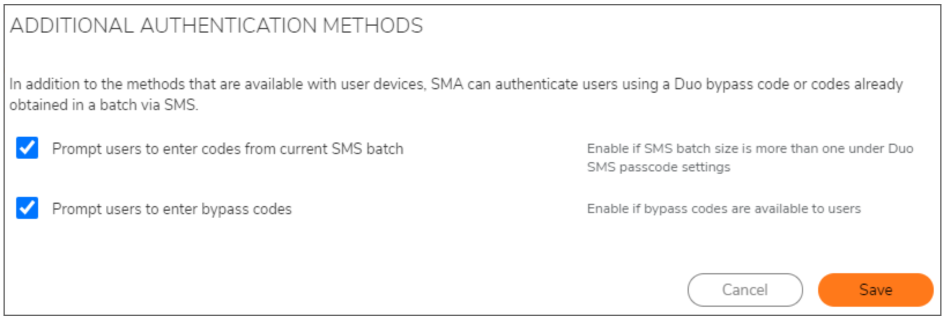
In addition to the methods that are available with user devices, SMA1000 can authenticate users using a Cisco Duo Security MFA bypass code or codes already obtained in a batch via SMS.

The batch code and bypass code options are configurable by admin as they are available in SMA1000 AMC.

> ⓘ **NOTE:** If these options are disabled, users will not see option to enter bypass codes and batch codes during login. Enable these only if application policy under Duo admin portal is configured to allow bypass codes and batch codes.

To use additional authentication methods do the following:

1. In the AMC, navigate to **System Configuration** > **Authentication Servers** > **Cisco Duo Security MFA**.
2. Under the **Additional Authentication Methods** section, select the following options:



ADDITIONAL AUTHENTICATION METHODS

In addition to the methods that are available with user devices, SMA can authenticate users using a Duo bypass code or codes already obtained in a batch via SMS.

☑ Prompt users to enter codes from current SMS batch — Enable if SMS batch size is more than one under Duo SMS passcode settings

☑ Prompt users to enter bypass codes — Enable if bypass codes are available to users

Enrollment method	Description
Prompt users to enter codes from current SMS batch	Enable if SMS batch size is more than one under Duo SMS passcode settings
Prompt users to enter bypass codes	Enable if bypass codes are available to users

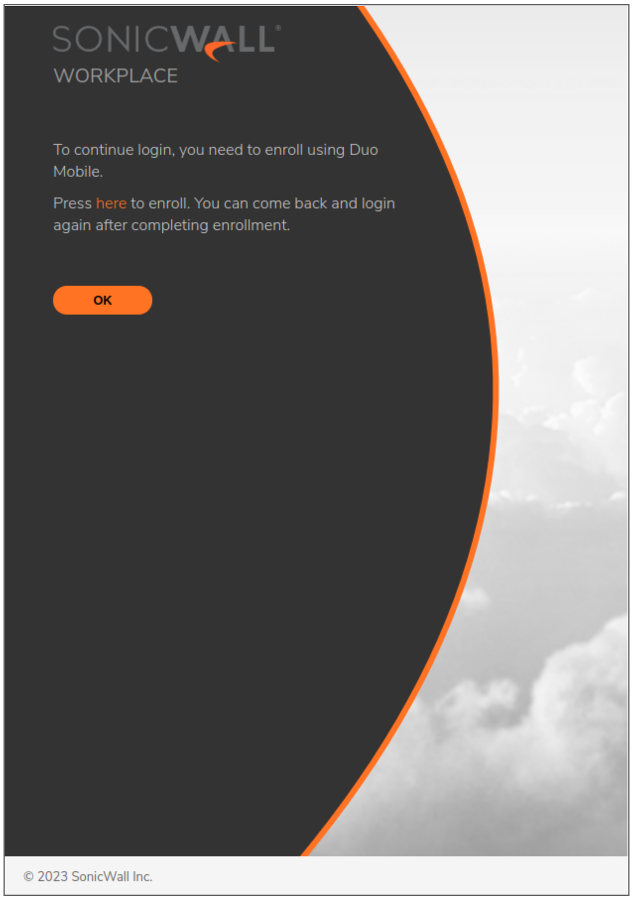
3. Click **Save.**

Some notes on Cisco Duo Security MFA server:

- Cisco Duo Security MFA sever can only be added as secondary authentication server under a realm.
- During user login, username entered by the user for primary server authentication should match with the username enrolled with Duo.
- If the format differs, for example when username entered by the user is "user@example.com" but Duo server lists just "user" without any domain name, change the "Username normalization" setting to "Simple" under application policy on Duo admin portal.
- Connect Tunnel clients installed on user devices should be upgraded to 12.4.3 and above for them to support Duo MFA server.

SMA1000 Clients and AMC Authentication Support

Cisco Duo Security Multi-Factor Authentication servers are supported by all the actively supported clients like Connect Tunnel (CT) on Windows/Mac/Linux platforms, and Workplace.



To continue login, you need to enroll using Duo Mobile.

Press here to enroll. You can come back and login again after completing enrollment.

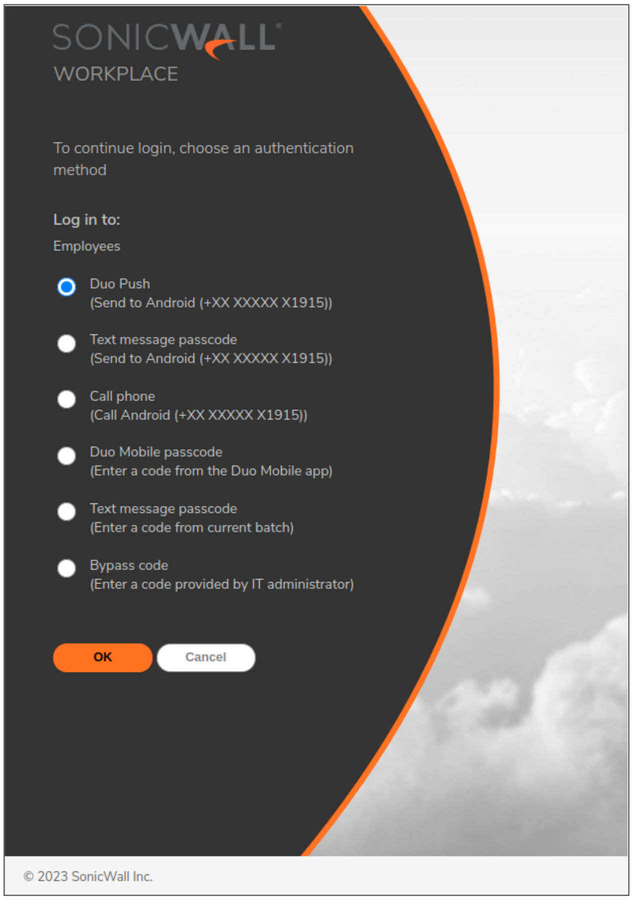
© 2023 SonicWall Inc.

SMA1000 AMC supports this authentication server for admin login and supports user enrollment as well.

Access methods like DeviceVPN, ActiveSync, and Outlook access do not support user-interaction and are forced to authenticate based on Duo's automatic authentication method. This means authentication happens via authentication methods like Push notification or phone call (if available for the user) without any interaction with user. User enrollment is not be supported for those access methods.

After you have integrated and configured SMA1000 with Cisco Duo Security MFA, when you log into clients like CT or Workplace you can:

1. Complete primary authentication. Select one of the MFA methods to authenticate.
   For example, if you have selected Duo Push and click **OK**, approve notification is sent to your device.



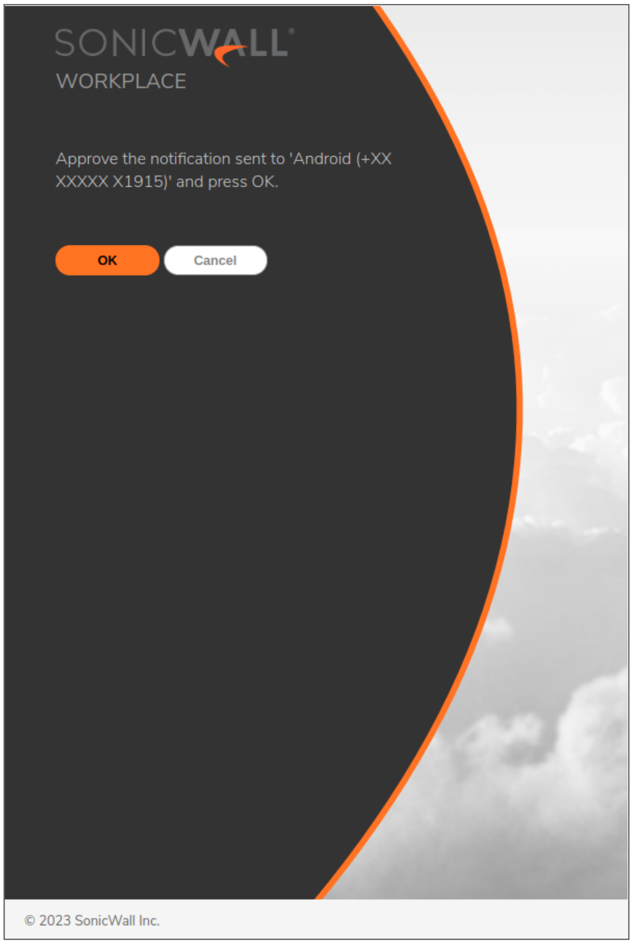
SONICWALL
WORKPLACE

To continue login, choose an authentication method

Log in to:
Employees

- ● Duo Push
  (Send to Android (+XX XXXXX X1915))
- ○ Text message passcode
  (Send to Android (+XX XXXXX X1915))
- ○ Call phone
  (Call Android (+XX XXXXX X1915))
- ○ Duo Mobile passcode
  (Enter a code from the Duo Mobile app)
- ○ Text message passcode
  (Enter a code from current batch)
- ○ Bypass code
  (Enter a code provided by IT administrator)

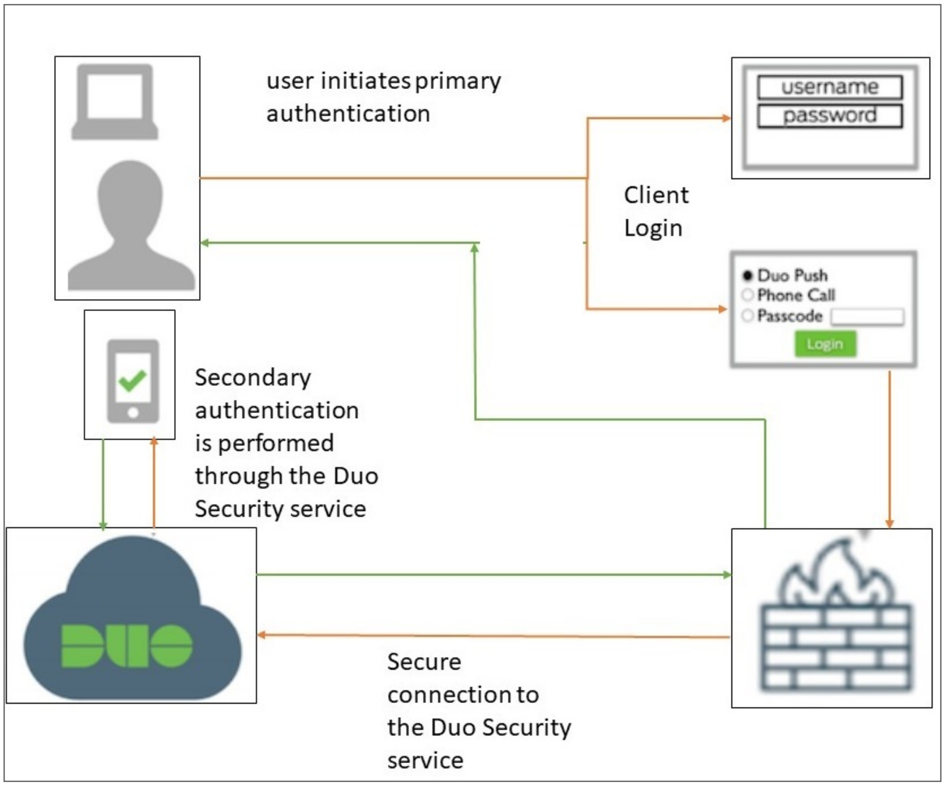
© 2023 SonicWall Inc.



Approve the notification sent to 'Android (+XX XXXXX X1915)' and press OK.

2. In order to change the MFA authentication method, click the **Cancel** button to go back and view the available authentication methods.
3. Enroll by redirecting the user to Duo enrollment portal if they are not already enrolled with Duo MFA server.

The workflow depicts the Cisco Duo Security MFA server service for a user :


user initiates primary authentication
username
password
Client Login
● Duo Push
○ Phone Call
○ Passcode
Login
Secondary authentication is performed through the Duo Security service
DUO
Secure connection to the Duo Security service

User-Mapped Tunnel Addressing

User-Mapped Tunnel Addressing enables network administrators to identify network traffic from a specific user by the source IPv4 address of the traffic.

On an internal network, administrators may sometimes be able to associate specific end users with specific IPv4 addresses, that are assigned to the user by the administrator.

Although assigning IP addresses to specific users is currently supported through the use of external RADIUS servers, User-Mapped Tunnel Addressing enables administrators to specify the assignment from an attribute in the appliance's local authentication server.

Administrators who deploy a RADIUS server as their authentication server can include an IPv4 address in the RADIUS Framed IP Address parameter for a specific user and associate that user's Community with a RADIUS address pool. This type of assignment can be done only if the address is available and no addressing conflicts prohibit it.

ⓘ **NOTE:** If an address conflict prevents this type of assignment, the normal tunnel addressing process continues with the next tunnel in the list that is allowed by the Community. If no more pools are available, the tunnel configuration fails.

The RADIUS Pool in the Configure Network Tunnel Service is now called the User-Mapped Pool. When a RADIUS-framed IP address is available from the authentication server, that address is available to the

User-Mapped Pool. An IPv4 address that is provided by a user’s local authentication server, is also available to the User-Mapped Pool and is used exactly the same as if it was from the RADIUS Pool. The User-Mapped Tunnel Addressing feature extends user-mapped addresses to the local user’s authentication server. No other address pools may supply addresses.

More than one address may be obtained from the authentication server, enabling a single user to establish more than one tunnel simultaneously, on separate devices. The number of simultaneous tunnel connections that a single user can establish can be configured by specifying the number of addresses for a user in the authentication server. This value can also be configured by setting the **Maximum Active** Sessions limit for all users of a particular community on the **Configure Community** page.

The User-Mapped Tunnel Address Pool, like RADIUS, can be used to provide a strict correspondence (or mapping) between virtual IPv4 addresses and tunnel clients. You can specify that a particular client gets a virtual address from a particular pool on the **Network Tunnel Client** Settings page. The client is assigned to a specific community and that community only gets IPv4 addresses from a particular address pool.

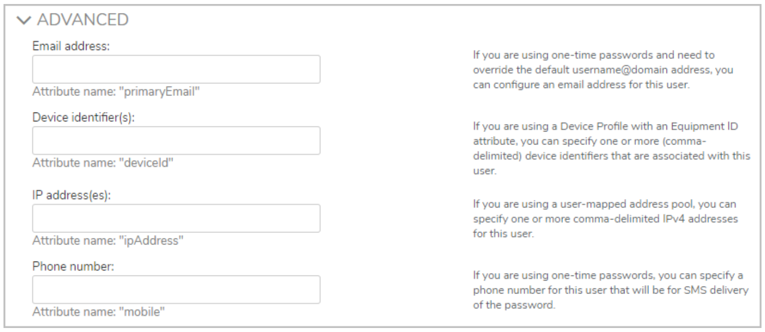
The User-Mapped Tunnel Address Pool attempts to establish an IPv4 address as the tunnel virtual address at tunnel connect time. If the address is available and no client-side conflicts arise, the virtual address is assigned. If the address fails, then the system proceeds to the next address pool in the list allowed by the community. If no other address pools are available, the tunnel connection attempt fails.

The authentication server used to get IPv4 addresses is not limited to its own authentication server. The User-Mapped Tunnel Address Pool may get addresses from its own authentication server or from the client’s local authentication server.

The authentication server may supply an ordered list of IPv4 addresses, not just a single address, so that you can assign multiple simultaneous tunnel connections to a single client, on separate devices.

On the **Security Administration > Users & Groups** page, on the **Add Local User** page, under the **Advanced** section, you can configure the following fields:

- Email address
- Device identifier(s)
- IP address(es)



ADVANCED

Email address:

Attribute name: "primaryEmail"

If you are using one-time passwords and need to override the default username@domain address, you can configure an email address for this user.

Device identifier(s):

Attribute name: "deviceId"

If you are using a Device Profile with an Equipment ID attribute, you can specify one or more (comma-delimited) device identifiers that are associated with this user.

IP address(es):

Attribute name: "ipAddress"

If you are using a user-mapped address pool, you can specify one or more comma-delimited IPv4 addresses for this user.

Phone number:

Attribute name: "mobile"

If you are using one-time passwords, you can specify a phone number for this user that will be for SMS delivery of the password.

To edit local users information:

1. In the AMC, navigate to **Security Administration > Users & Groups**.
2. Click **Local Accounts** and then click on the **Name** of the local account you want to edit.

3. Expand the **Advanced** section to access the additional options.
4. In the **Email Address** field, configure an email address for the user. This address is used for sending one-time passwords to the user, and overrides the default `username@domain` email address. This email address is assigned to the "mail" attribute for the user.
5. In the **Device identifier(s)** field, enter one or more (comma-delimited) device identifiers for computers or other devices that are associated with this user.
6. In the IP address(es) field, enter either a single IPv4 address or list of IPv4 addresses (comma-delimited). If you enter a:
    - Single IPv4 address, each IPv4 address should match the network address of the resource interface.
    - List of IPv4 addresses, these addresses are presented to the User-Mapped Tunnel Address Pool, in the order they appear in the list.

Integration of SMA1000 with RSA SecurID Authentication Manager

RSA SecurID Authentication Manager is a multi-factor authentication solution that verifies authentication requests and centrally administers authentication policies for enterprise networks. Authentication Manager can manage security tokens, users, multiple applications, agents, and resources across physical sites, and to help secure access to network, Cloud, and web-accessible applications.

By integrating RSA SecurID Authentication Manager with SMA1000 acts as an agent to RSA Authentication Manager and leverages its authentication services.

Topics:

- Configuring RSA Server Authentication
- Configuring the RSA SecurID Authentication Manager
- SMA1000 Clients and AMC Authentication support

Configuring RSA Server Authentication

The appliance supports SecurID, token-based user credentials that are validated against a database on an RSA Authentication Manager (Legacy) server. Configuring this type of authentication involves changes on both the RSA server and the SMA appliance, which are outlined below. Affinity servers should be used only for authentication servers that do not include full group search capabilities, such as RADIUS, RSA, and PKI servers.

ⓘ **NOTE:** If you are using the latest RSA SecurID Authentication Manager using the SecurID Authentication API, then you

can skip this section and go to Configuring the RSA SecurID Authentication Manager.

To configure RSA Authentication Manager for token-based credentials:

1. Create an agent host on the RSA server with the IP address for the internal interface of the SMA appliance.
2. Make the configuration changes necessary to resolve the names of both the RSA server and the SMA appliance:
    - DNS must be able to resolve the RSA server's name; simply adding the appliance and its IP address to your `/etc/hosts` file will not work.
    - The appliance's name (as configured on the RSA server) must resolve to the internal IP address of the appliance.
3. DNS must be able to resolve the RSA server's name in both directions:
    - The appliance's name (as configured on the RSA server) must resolve to the internal IP address of the appliance; simply adding the appliance and its IP address to your `/etc/hosts` file will not work.
    - The RSA server requires a reverse DNS entry for the internal interface of the SMA appliance.
4. After adding the agent host on the RSA server, make sure that you generate the configuration file (`sdconf.rec`) for the correct agent host.
5. In the AMC, navigate to **System Configuration > Authentication Servers**.
6. Click **New**.
7. Select **RSA Authentication Manager (Legacy)**.
8. In the **Name** field, type a name for the authentication server.
9. Specify the location of your RSA Authentication Manager (Legacy) server SecurID configuration file, `sdconf.rec`. This configuration file is in binary format and contains the ports and processes associated with the RSA authentication service. When in place, this file is used by the RSA libraries to communicate over the network to an RSA server.
10. Click **Save** to upload it to the appliance.
11. The node secret is negotiated when the first authentication request is made from the agent host. Make sure that the **node secret created** flag is cleared on the RSA server.

ⓘ | **NOTE:**

- If you make any changes to the RSA server (for example, change its IP address, host name, or re-install it), the `sdconf.rec` file must be uploaded to the appliance again.
- After upgrading some older versions, users may not be able to authenticate through the RSA server because the node secret did not migrate properly. In this case, clear the node secret for the authentication agent on the RSA server.

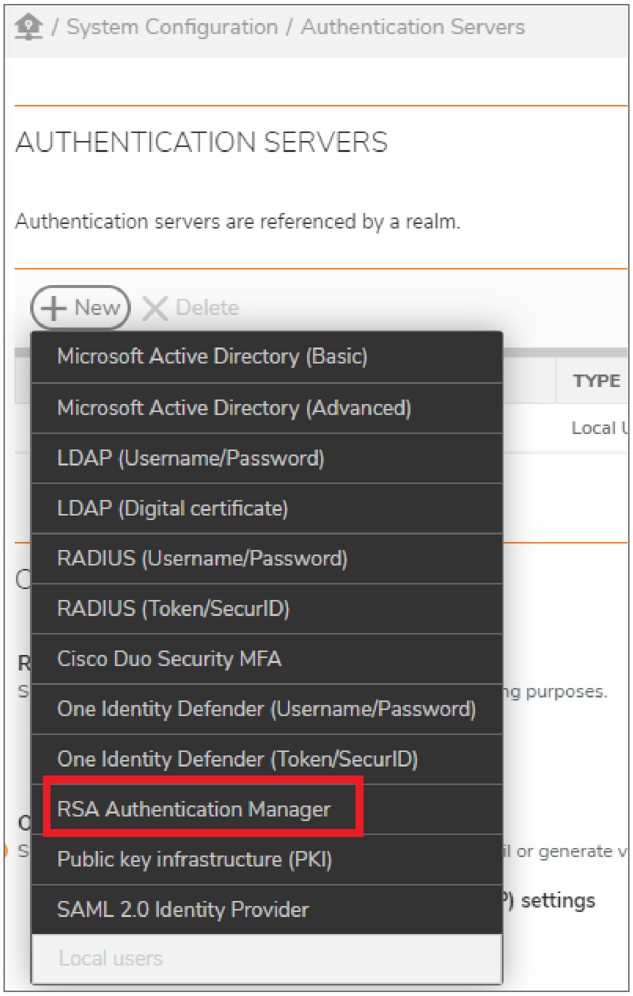
Configuring the RSA SecurID Authentication Manager

Prerequisites:

- SMA1000 running 12.4.3 firmware version.
- You must be running RSA Authentication Manager 8.2 SP1 or later to access this interface. The steps are summarized in this section; see your RSA Security Console documentation for complete details.

To configure RSA SecurID Authentication Manager, do the following:

1. Open the RSA Security Console.
   a. Select **Setup** > **System settings** > **RSA SecurID Authentication API** .
   b. Select the **Enable Authentication API** check box.
   c. Note the values for the **Access ID** and **Access Key**.
   d. (Optional) In the **Communication Port** field, enter the port number the AMC will use to communicate with the RSA SecurID Authentication API. The default is 5555.
   e. Click **Apply Settings**. See RSA Authentication Manager Setup configuration guide for more details.
2. In SMA1000 AMC appliance, navigate to **System Configuration** > **Authentication Servers**.
3. Click **New** and select **RSA Authentication Manager**.



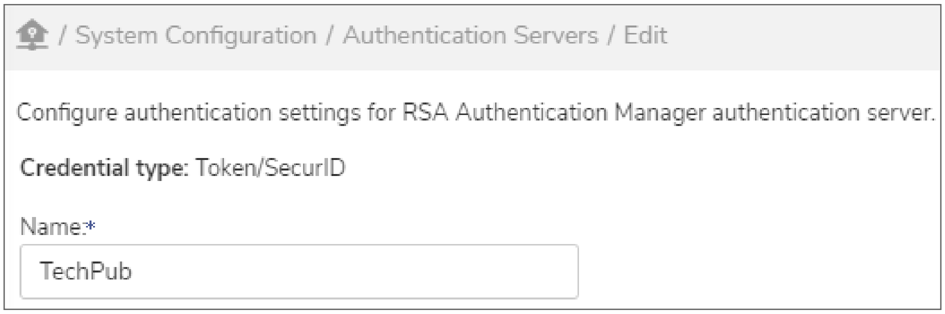
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

+ New
Delete
TYPE
Local U
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
ng purposes.
il or generate v
) settings

4. In the **Name** field, type a name for the authentication server profile.



/ System Configuration / Authentication Servers / Edit

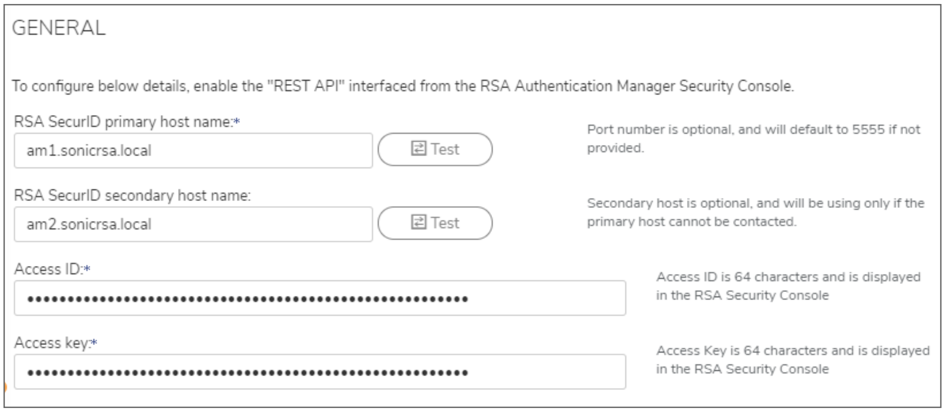
Configure authentication settings for RSA Authentication Manager authentication server.

Credential type: Token/SecurID

Name:*

TechPub

5. Under the **General** section:



GENERAL

To configure below details, enable the "REST API" interfaced from the RSA Authentication Manager Security Console.

RSA SecurID primary host name:* am1.sonicrsa.local

Port number is optional, and will default to 5555 if not provided.

RSA SecurID secondary host name: am2.sonicrsa.local

Secondary host is optional, and will be using only if the primary host cannot be contacted.

Access ID:* ••

Access ID is 64 characters and is displayed in the RSA Security Console

Access key:* ••

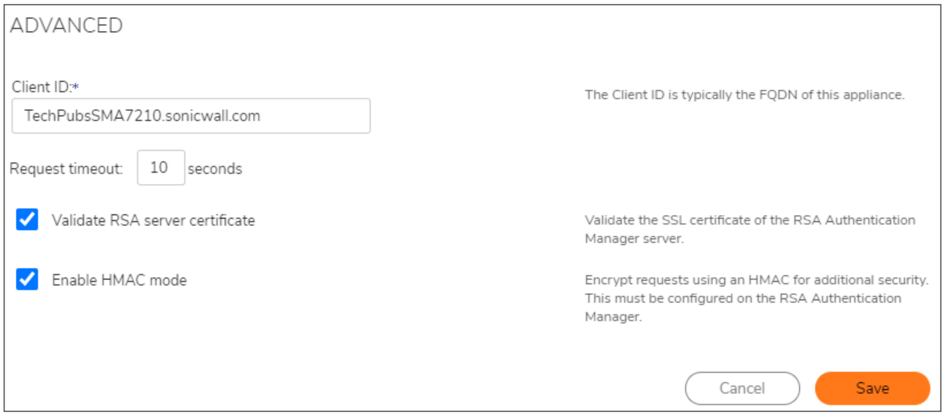
Access Key is 64 characters and is displayed in the RSA Security Console

a. Enter the host name in **RSA SecurID primary host name**. It is typically an IP Address or FQDN. The default value of port is 5555.

b. Enter the host name in **RSA SecurID secondary host name**. It is typically an IP Address or FQDN. The secondary host name is used only if the primary host cannot be contacted.

c. Enter the **Access ID** and **Access key** copied from RSA Security Console portal. The keys are of 64 characters.

6. Under the **Advanced** section:



ADVANCED

Client ID:* TechPubsSMA7210.sonicwall.com

The Client ID is typically the FQDN of this appliance.

Request timeout: 10 seconds

☑ Validate RSA server certificate

Validate the SSL certificate of the RSA Authentication Manager server.

☑ Enable HMAC mode

Encrypt requests using an HMAC for additional security. This must be configured on the RSA Authentication Manager.

a. Enter the Authentication Agent name for the AMC appliance that you configured in the RSA Authentication Manager. **Client ID**. By default the FQDN is auto filled in text box.

b. If required change the **Request timeout**.

It is the amount of time the connection between AMC appliance server and the RSA server can remain inactive before the session times out. The default is 10 seconds. The minimum is 5 seconds and maximum is 60 seconds.

c. Enable the **Validate RSA server certificate** to validate the SSL certificate of the RSA Authentication Manager server. By default it is disabled.

d. Select **Enable HMAC mode** to encrypt authentication requests, enabled or configured in RSA Security Console portal.

The administrator can generate a Hash-based Message Authentication Code (HMAC) that can be used to encrypt authentication requests between SMA1000 and the RSA SecurID Authentication API. The HMAC provides a hash for the request body and an HMAC signature. For more information you can refer to Generate an HMAC for Authentication Agents guide.

7. Click **Save**.
8. Create Realm to add a RSA SecurID Authentication Manager server as a primary or secondary authentication server. For more information refer to Configuring Chained Authentication

SMA1000 Clients and AMC Authentication support

The RSA SecurID authentication servers are supported by all the actively supported client like Connect Tunnel (CT) on Windows/Mac/Linux platforms, and Workplace.

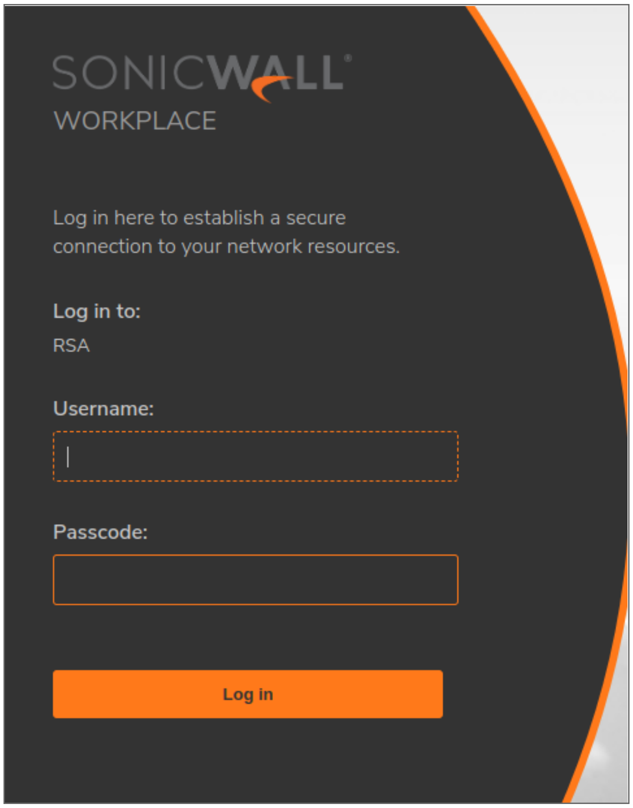
Access methods like DeviceVPN, ActiveSync, and Outlook access cannot use RSA AM authentication.

After you have configured the RSA SecurID authentication server, when you log to CT or Workplace you can:

1. User initiates primary authentication by entering the username and Passcode.

   The client displays the user provided Passcode and pass it to RSA Authentication Manager for validation.

   A SecurID Passcode is the combination of a PIN and token code. Similar to the token code, a Passcode is a one-time password (OTP). It is valid only while it is displayed, and it can be used only once. The SecurID Passcode consists of your PIN followed by the token code and you must enter both. For example, if your PIN is 1234 and the token code is 567891, you enter the Passcode as 1234567891.



SONICWALL

WORKPLACE

Log in here to establish a secure connection to your network resources.

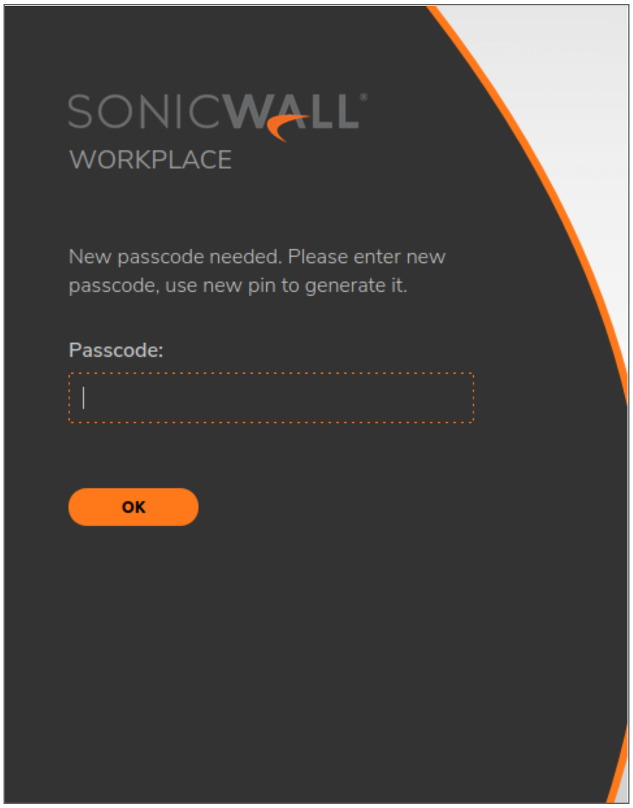
Log in to:
RSA

Username:

Passcode:

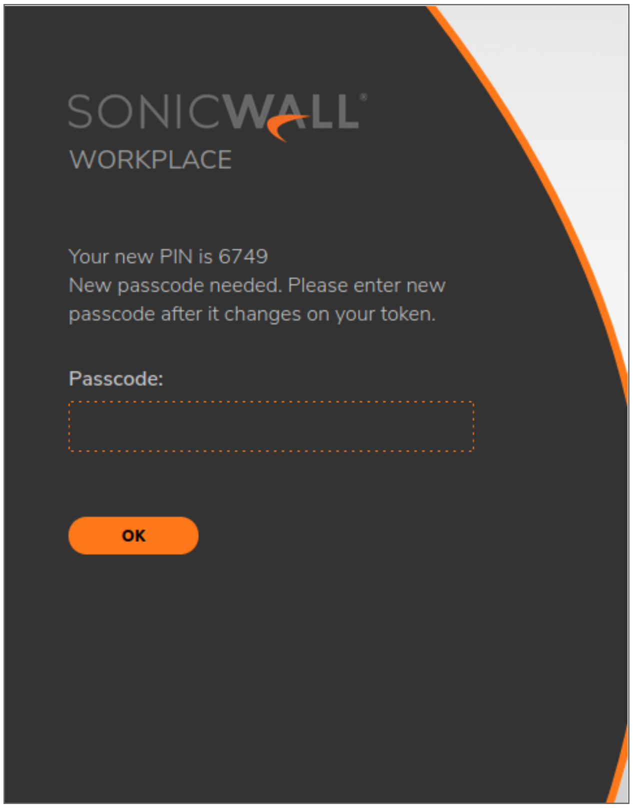
2. RSA Authentication Manager requests the next Passcode in case the user exceeds previous wrong attempts more than set policy count. Thus enforcing to change Passcode. The Passcode can be a combination of Pin+Token or only Token based on how it was configured on RSA Security console to authenticate.

   The client displays to change the user's Passcode and to use new pin generated by the authentication server. The token generates a new Passcode at regular intervals, typically every 60 seconds. You then use the generated Passcode when you log in.



New passcode needed. Please enter new passcode, use new pin to generate it.

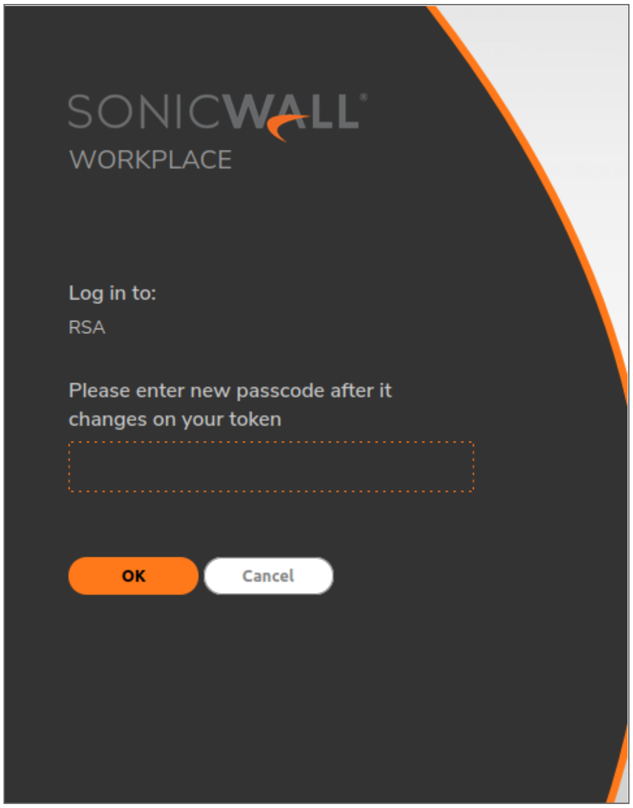
Passcode:



Your new PIN is 6749
New passcode needed. Please enter new passcode after it changes on your token.

Passcode:

3. Enter the next Passcode to complete the login.



Log in to:

RSA

Please enter new passcode after it changes on your token

Configuring a PKI Authentication Server

You can set up a certificate server so that a user authenticates using a client certificate on his or her device. Digital certificate authentication can be used alone or in conjunction with another authentication method, such as RADIUS. (If you set up chained authentication and a digital certificate is one of the methods you use, it must be the first method; for more information, see Configuring Chained Authentication.)

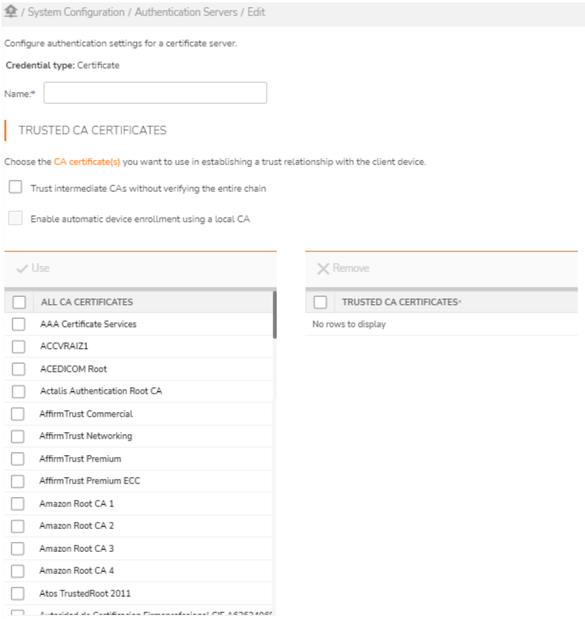
ⓘ **NOTE:** Affinity servers should be used only for authentication servers that do not include full group search capabilities, such as RADIUS, RSA, and PKI servers.

ⓘ **NOTE:**

- If both CRL and OCSP are enabled for a CA certificate, only OCSP is used.
- Fallback from CRL to OCSP or OCSP to CRL is not supported.

To configure a PKI authentication server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.
3. Click **Public key infrastructure (PKI)**.



/ System Configuration / Authentication Servers / Edit

Configure authentication settings for a certificate server.

Credential type: Certificate

Name:*

TRUSTED CA CERTIFICATES

Choose the CA certificate(s) you want to use in establishing a trust relationship with the client device.

□ Trust intermediate CAs without verifying the entire chain

□ Enable automatic device enrollment using a local CA

□	ALL CA CERTIFICATES
□	AAA Certificate Services
□	ACCVRAIZ1
□	ACEDICOM Root
□	Actalis Authentication Root CA
□	AffirmTrust Commercial
□	AffirmTrust Networking
□	AffirmTrust Premium
□	AffirmTrust Premium ECC
□	Amazon Root CA 1
□	Amazon Root CA 2
□	Amazon Root CA 3
□	Amazon Root CA 4
□	Atos TrustedRoot 2011
□	Autoridad de Certificacion Firmaprofesional CIF A6263406

□	TRUSTED CA CERTIFICATES*
	No rows to display

4. In the **Name** field, type a name for the authentication server.

5. Under **Trusted CA certificates**, optionally

   - Select the **Trust intermediate CAs without verifying the entire chain** checkbox. This allows a set of trusted intermediate signing authority certificates to be deployed in various sectors of the network (often by department or organizational unit). For more information, see About Intermediate Certificates.

   - Select the **Enable automatic device enrollment using a local CA** checkbox only for PKI with local CA and not for any other CA.

6. Under **Use** is a list of **All CA certificates** used by the appliance. Select one or more root certificates for establishing a trust relationship with the client device by selecting the checkbox (a root certificate is one where the **Subject** and **Issuer** are the same). A client's certificate will be trusted if it matches a root certificate listed in the **Trusted CA certificates** list.

7. Under **Advanced**, in the **Username attribute** field, type the attribute used for single sign-on (for example, `cn` or `uid`).

8. To use an OCSP responder to determine client certificate status, select the **Use OCSP to verify client certificates** checkbox. If selected, a user may use any access method (Workplace or Connect Tunnel) to authenticate to a realm that uses this PKI authentication method.

9. Select one of the following options for **Use this OCSP responder**:

   - **System default** – A manually configured OCSP responder has priority. The configured OCSP responder URL is shown here if configured. You can configure it by clicking the **here** link, which takes you to the **OCSP** page available from **SSL Settings**.

   - **User certificate's AIA extension** – The user certificate is parsed to extract the URL of the OCSP responder. The Authority Information Access (AIA) certificate extension contains URL locations that provide the issuing CA's certificate. The AIA extension can contain HTTP, FTP, LDAP, or FILE URLs.

- **CA certificate's AIA extension** – The CA certificate is parsed to extract the URL of the OCSP responder.

10. Select the **Allow certificate if responder is unavailable** checkbox if the authentication should succeed in cases where an error occurs, an **unknown** status is returned, or the OCSP responder is not available.
11. Select the **Trust signing certificates in response** checkbox to trust certificates in the OCSP response. This is enabled by default.

    You must import the OCSP response signing certificate for the CA certificate being used and enable **OCSP response verification** when importing it. The OCSP response signing certificate can be copied from the OCSP responder or server to a local management machine and then imported from the **SSL Settings** page while you are logged in to AMC.
12. Select the **Send nonce in request** checkbox and **Require nonce in response** checkbox to guard against malicious replay attacks, in which a successful response is replayed to the client after the subject certificate is revoked.
13. Click **Save**.

Additional Field for Custom Certificates

The custom SSL client certificate has an additional field to contain an employee ID number (a 10-digit number). This employee ID number can be parsed and passed to an Active Directory authentication server, which will use this additional information to determine the authorization and client access privilege of the client and add that client to the authorized group.

To generate and gain access to SMA with a custom certificate:

1. Create a custom certificate; include the Employee ID number in the custom field.
2. Create a user group on the Active Directory authentication server based on the Employee ID number field.
3. Create an SMA access policy for that user group on the Active Directory authentication server.
4. Configure the Employee ID number field as the SSO username on the Active Directory authentication server.
5. Configure Group Affinity Checking on the Active Directory authentication server.
6. Add the appropriate resources and enable SSO for the configured username.

    The custom certificate is assigned to the client with that username and is installed on the client's device. The client can now use that device to access SMA and all resources that are enabled with SSO for that client.

Configuring a SAML-Based Authentication Server

Security Assertion Markup Language (SAML) is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML provides a foundation for Web based single sign-on

(Web SSO) by allowing business entities to make assertions regarding the identity, attributes, and entitlements of a subject (such as a human user) to other entities, such as a partner company or another enterprise application.

In Web SSO, a user either accesses a resource via a service provider (such as the SMA appliance), or accesses an identity provider (IDP) such that the service provider and desired resource are understood or implicit. The user authenticates to the IDP, which then produces an authentication assertion and the service provider consumes the assertion to establish a security context for the user. When the security context for the user exists, the user can access resources at another site without additional authentication. SAML also provides a Single Logout (SLO) service.

This release supports external IDPs that are deployed in the public Internet. It is assumed that the user uses a standard browser and can authenticate to the IDP by some means outside the scope of SAML. The user accesses the appliance through a SAML Authenticated Realm.

Configuring a SAML 2.0 Identity Provider Authentication Server

NOTE: For detailed information on how to configure third party SAML Identity Providers (IDPs), see Configuring External SAML Identity Providers.

SAML 2.0 Identity Provider (IDP) provides a centralized security management foundation that enables the secure use of the Web to deliver applications and cloud services to customers, partners, and employees.

SAML 2.0 Identity Provider Authentication supports all SAML 2.0-compliant IdPs, including:

- Microsoft Azure IDP
- Duo Access Gateway and Duo SSO server
- Okta
- One Identity Cloud Access Manager
- Shibboleth IDP
- OneLogin
- CA Single Sign-On (CA SiteMinder)
- PingIdentity PingOne

To ease configuring SAML endpoints, SMA supports configuration using SAML metadata files. This removes the complexity involved in manually configuring the endpoints. SAML IdP Authentication server configuration can be exported as SAML SP metadata file which then can be imported at IdP. Similarly, SAML metadata file provided by IdP can be imported to configure SAML IdP Authentication server. For more details, refer to Identifier Provider Configuration steps below.

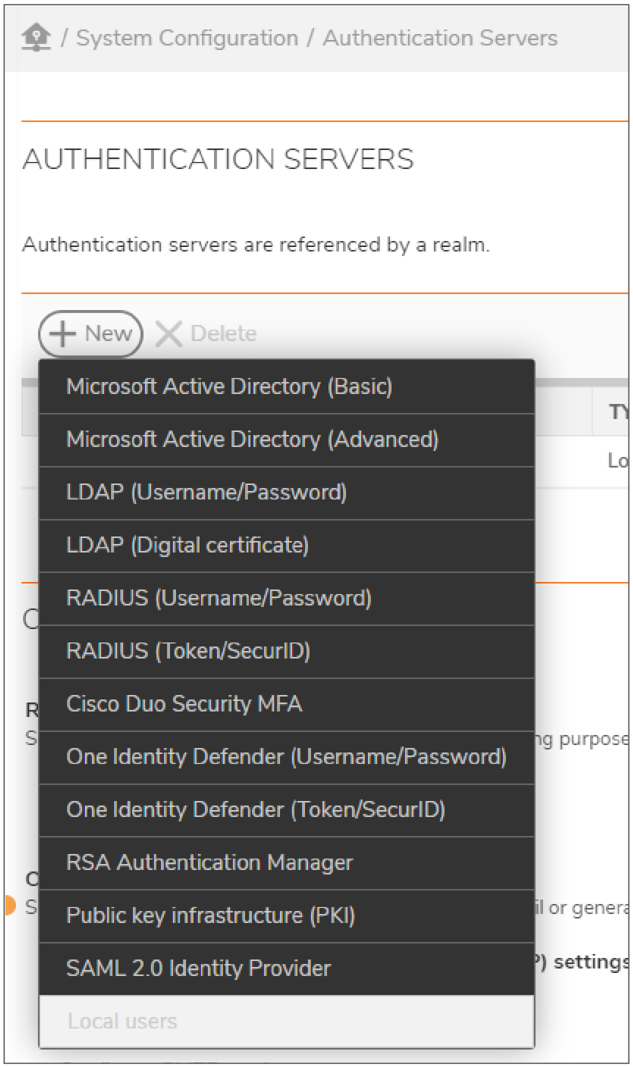
SMA and CMS is enhanced to support SAML authentication for Administrators. Also, SMA is enhanced to support group membership details over SAML authentication and users without on-premise Active Directory can now have group-based policy level management.

Prerequisites:

- SMA1000 build 12.4.1 version.
- SMA1000 Standalone/CMS platforms
- Admin account on any SAML IDP

To configure a SAML 2.0 Identity Provider authentication server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.



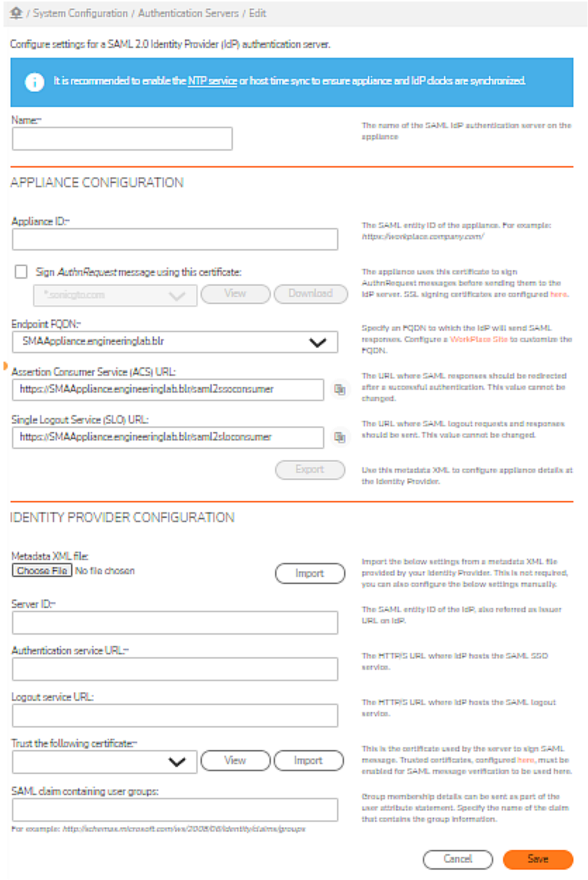
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users

3. Click **SAML 2.0 Identity Provider**.



/ System Configuration / Authentication Servers / Edit

Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

It is recommended to enable the NTP service or host time sync to ensure appliance and IdP clocks are synchronized.

Name:* — The name of the SAML IdP authentication server on the appliance

APPLIANCE CONFIGURATION

Appliance ID:* — The SAML entity ID of the appliance. For example: https://workplace.company.com/

□ Sign *AuthnRequest* message using this certificate: *.sonicgto.com — The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN:* SMAAppliance.engineeringlab.blr — Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

Assertion Consumer Service (ACS) URL: https://SMAAppliance.engineeringlab.blr/saml2ssoconsumer — The URL where SAML responses should be redirected after a successful authentication. This value cannot be changed.

Single Logout Service (SLO) URL: https://SMAAppliance.engineeringlab.blr/saml2sloconsumer — The URL where SAML logout requests and responses should be sent. This value cannot be changed.

Export — Use this metadata XML to configure appliance details at the Identity Provider.

IDENTITY PROVIDER CONFIGURATION

Metadata XML file: Choose File No file chosen — Import — Import the below settings from a metadata XML file provided by your Identity Provider. This is not required, you can also configure the below settings manually.

Server ID:* — The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:* — The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL: — The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:* — This is the certificate used by the server to sign SAML message. Trusted certificates, configured here, must be enabled for SAML message verification to be used here.

SAML claim containing user groups: — Group membership details can be sent as part of the user attribute statement. Specify the name of the claim that contains the group information.

For example: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

4. In the **Name** field, type a name for the authentication server.

5. In the **Appliance ID** field, enter the SAML entity ID of the appliance.

   This is a URI of not more than 1024 characters in length.

6. Select the **Sign AuthnRequest message using this certificate** checkbox and then select the signing certificate from the drop-down menu. The appliance uses this certificate to sign authentication request messages before sending them to the IDP server. To configure the SSL signing certificate, you can click the **here** link in the explanatory text at the right. The signing certificate needs to be imported into the appliance if it is not there. You can view and download the certificate by clicking on the respective buttons.

7. To specify an FQDN to which the IdP will send SAML responses, select the **Endpoint FQDN** from the drop-down menu.

8. The **Assertion Consumer Service (ACS) URL** and **Singel Logout Service(SQL) URL** fields displays the appliance endpoints. This value cannot be changed. You can click the copy icon to copy the URLs and paste in SAML IDP application.

   - ACS URL is where SAML responses should be sent after a successful authentication.
   - SLO URL is where logout requests should be redirected during IdP logout.

9. Click **Export** to use this metadata XML to configure appliance details at the Identity Provider.

10. To configure Identity Provider details underr **Identity Provider Configuration** section, you can either import the metadata file provided by your SAML IdP or you can fill in the details manually.

    - To import the metadata file from IdP do the following:

        a. Click on **Choose file** button and select the metadata file.

        b. Click **Import** button to import the IdP configuration details.

        Identity Provider fields are populated.

    - To fill in the configuration details manually do the following:

        a. In the **Server ID** field, enter the **SAML Entity ID** of SAML IdP. For example, *https://idp.example.com/*.

        b. In the **Authentication service URL** field, enter the **SAML Single Sign-On Service URL** provided by IdP.

        c. In the **Logout service URL** field, enter the **Sign-Out URL** provided by IdP. This field is optional and can be left empty.

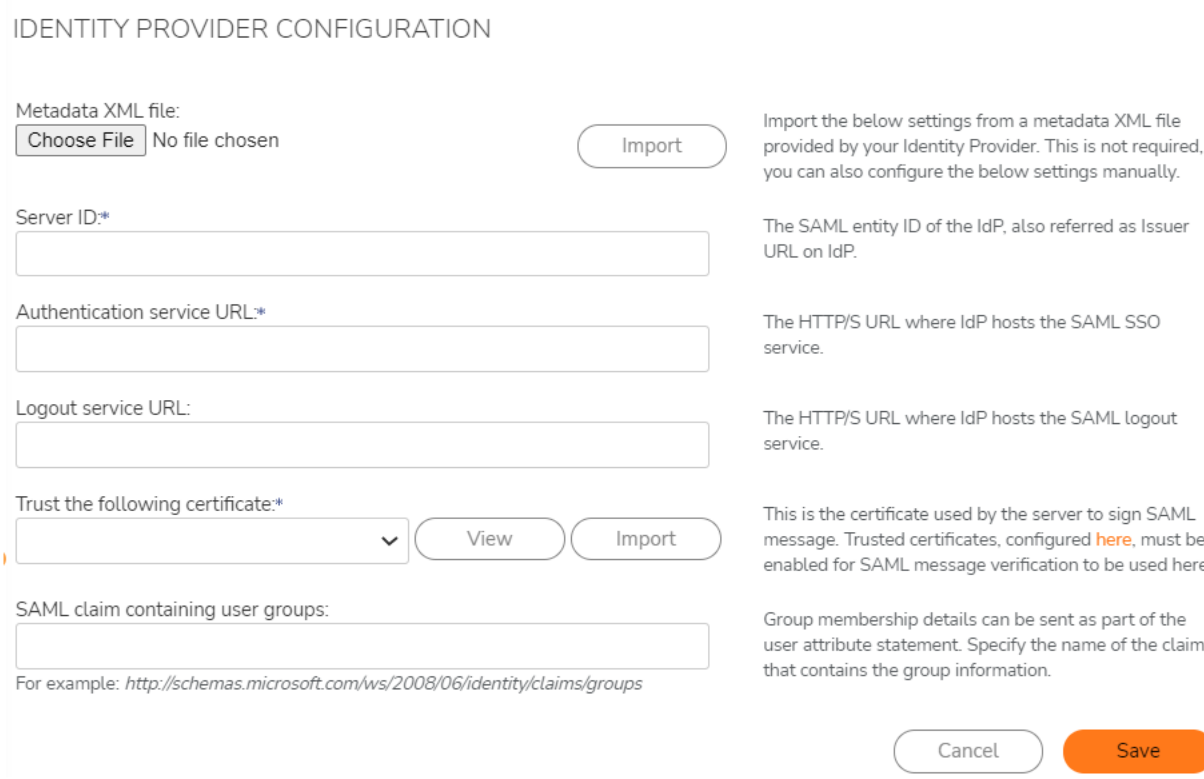
        ⓘ **NOTE:** The **Logout service URL**' field is optional and can be left empty. When provided, when user is logging out of SMA, user will be redirected to the given URL with SAML logout request, effectively logging out the user from IdP. Clear this field if you dont want user to log out from IdP when logging out from SMA.

        d. From the **Trust the following certificate** drop-down menu, select the certificateprovided by IdP. If the certificate is not listed, use 'Import' button to import it.

        e. SMA supports group membership details over SAML authentication and users without on-premise Active Directory can now have group level management. In the **SAML claim containing user groups** field, specify the name of the claim that contains the group information. For example: *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*.

        - ⓘ **NOTE:** The **SAML claim containing user groups** field is configured with user group attribute name, for more information, refer to the Group Management with SAML IdP

ⓘ | authentication server section.



IDENTITY PROVIDER CONFIGURATION

Metadata XML file: No file chosen

Import the below settings from a metadata XML file provided by your Identity Provider. This is not required, you can also configure the below settings manually.

Server ID:*

The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:*

The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL:

The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:*

This is the certificate used by the server to sign SAML message. Trusted certificates, configured here, must be enabled for SAML message verification to be used here

SAML claim containing user groups:

For example: *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*

Group membership details can be sent as part of the user attribute statement. Specify the name of the claim that contains the group information.

11. Click **Save**.

ⓘ | **NOTE:** Follow the same procedure to configure SAML IDP authentication in CMS.

Group Management with SAML IdP authentication server

When SAML IdP is used as the authentication server for users, there are two ways to have the group level management.

Topics:

- Using Group Affinity checking
- Using SAML Attributes during authentication

Using Group Affinity checking

If the same Active Directory used by IdP is available on-premise, you can configure it as an authentication server and use it as Group Affinity server under SAML IdP realm. In this case, SMA will use SAML IdP to authenticate users and on-premise Active Directory for group checking. For more details on how to add Group Affinity, see Enabling Group Affinity Checking in a Realm

After enabling Group Affinity for SAML IdP realm, you can add "Mapped Accounts" by "Browse Directory" or "Dynamic Group" options and selecting SAML IdP realm.

Using SAML Attributes during authentication

In situations where group membership details are available only with IdP (cloud-only directories) or when on-premise Active Directory server is not available, SMA can recognize user-groups sent as SAML Attribute by IdP during authentcation.

Topics:

- Configure SAML IdP
- Update SMA SAML IdP authentication server

Configure SAML IdP

You will need to modify SAML IdP server to send user's group membership details as SAML Attributes to SMA. Note down the SAML Attribute/claim name that carries the user-group list.

For details on how to send User Groups, see Sending User Groups to SMA.

Update SMA SAML IdP authentication server

Under **Identity Provider Configuration** section, in "SAML claim containing user groups" field, add the SAML Attritbute name containing user-groups.

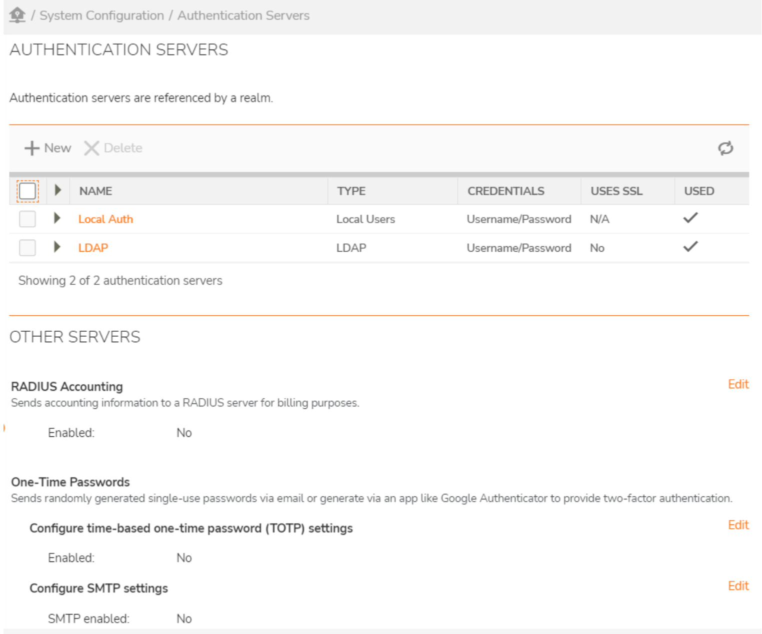
To configure User Group details, see Adding Users or Groups Manually.

One Identity Defender

Defender is a product for 2-factor authentication. SMA supports One Identity Defender configuration as a generic RADIUS server.

To configure a new Authentication Server with One Identity Defender:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

	NAME	TYPE	CREDENTIALS	USES SSL	USED
□	Local Auth	Local Users	Username/Password	N/A	✓
□	LDAP	LDAP	Username/Password	No	✓

Showing 2 of 2 authentication servers

OTHER SERVERS

RADIUS Accounting Edit

Sends accounting information to a RADIUS server for billing purposes.

Enabled: No

One-Time Passwords

Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

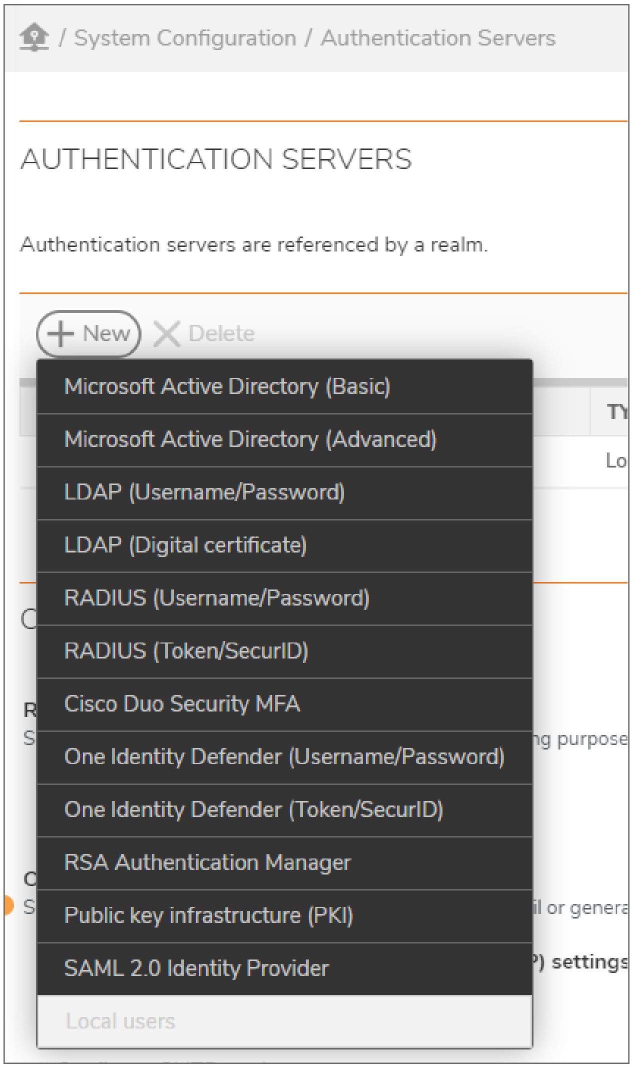
Configure time-based one-time password (TOTP) settings Edit

Enabled: No

Configure SMTP settings Edit

SMTP enabled: No

2. Click on **New**.



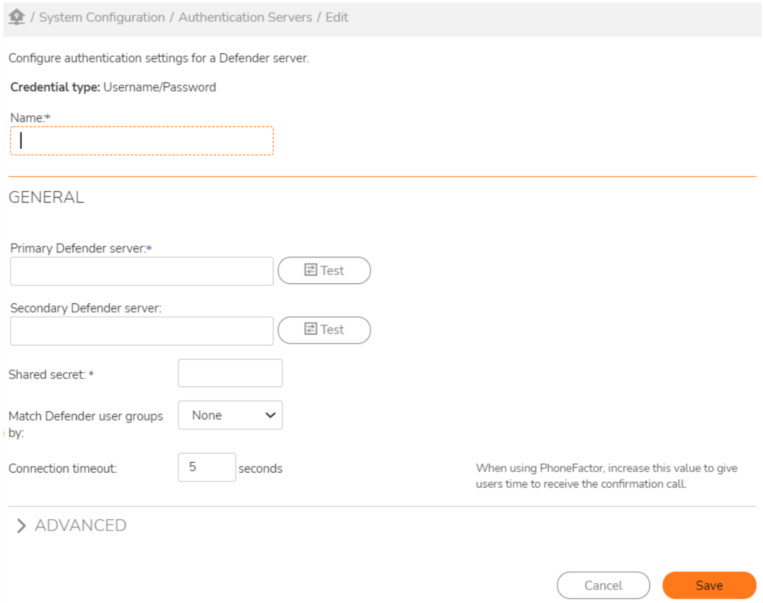
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users

3. Select the **One Identity Defender** option.


/ System Configuration / Authentication Servers / Edit
Name:*
GENERAL
Primary Defender server:*
Test
Secondary Defender server:
Test
Shared secret: *
ADVANCED
Cancel
Save

Configure authentication settings for a Defender server.

Credential type: Username/Password

Match Defender user groups by: None

Connection timeout: 5 seconds

When using PhoneFactor, increase this value to give users time to receive the confirmation call.

4. In the **Name** field, enter a name for the authentication server.
5. In the **Primary Defender server** field, enter the IP address of the primary defender server.
6. In the **Secondary Defender server** field, enter the IP address of the secondary defender server.
7. In the **Shared Secret** field, enter your shared secret.
8. From the **Match Defender user groups by** drop-down menu, select:
   - **None** (default)
   - **filterid attribute (11)**
   - **class attribute (25)**
9. In the **Connection timeout** field, enter the connection timeout value, in seconds.
10. Click **Save**.

Configuring Local User Storage

You can create local user accounts in AMC and then map them to a local authentication repository. For information on creating local user accounts, see Managing Local User Accounts.

Only one local user store can be created on the appliance.

To configure local user authentication:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **New**.
3. Click **Local users** (if a local store already exists, this option is dimmed).
4. In the **Name** field, type a name for the authentication server.

5. In the **Password policy** area, specify the minimum and maximum number of characters allowed for passwords. The minimum can be as few as 8, and the maximum can be as many as 12.

Option	Description
Lowercase	To specify that user passwords must contain at least one lowercase character
Uppercase	To specify that user passwords must contain at least one uppercase character.
Numeric digits (9-0)	To specify that user passwords must contain at least one number (0-9).
Symbols	To specify that user passwords must contain at least one symbolic character (~`!@#$%^&*()_-+={}[]|\:;"'<,>.?/).

ⓘ | **NOTE:** UTF-8 characters are supported in the password.

6. In the **Password expiration** area, select the **Passwords expire after** checkbox. Clear the checkbox to allow user passwords to never expire.
   - Enter the number of days after which user passwords will expire. The default is 60 days ; minimum is 1 day, and the maximum is 365 days.
7. Select the **Begin prompting user** checkbox and enter the number of days before expiration that the user will be prompted to change the password. The default is **14** days.
8. To change the prompts and other text that Windows users see when they log in, expand the **Advanced** section.
9. Select the **Customize authentication server prompts** checkbox.

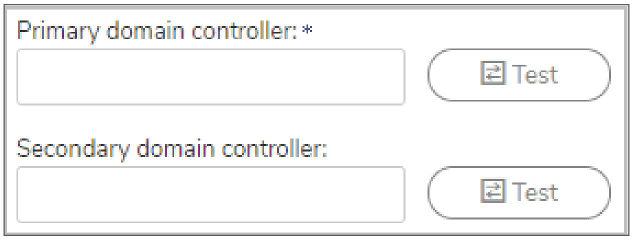
   The page title, message, and login prompts can all be customized. For example, if an employee ID number is used to identify a user, you could change the text for the **Identity** prompt from **Username** to **Employee ID**. If this configuration is being used for testing, a customized **Message** could point to test procedures or other instructions.
10. Enter the password or other proof of identity into the **Proof** field.
11. In the **One-Time Passwords area, to configure two-factor authentication with one-time passwords**, select **Use one-time passwords with this authentication server**.
12. Define the password format by entering the number and type of characters into the **Passwords contain** field.
13. In the **From address** field, enter the email address from which one-time passwords will be sent.
14. In the **Default domain** field, optionally enter the domain to be appended to each user name to create an email address for local users to which one-time passwords will be sent.
15. You can override the default domain by configuring an email address for each local user in the **Email Address** field.

    This email address will be available as a User attribute type policy variable named `primaryEmail`. One email address per user is supported.
16. Click the **Send test message** button to send a test email message to verify that the message, password, and SMTP settings are correct.
17. In the **Subject** field, enter the text for the subject line when e-mailing the one-time password.

18. In the **Body** field, enter the content of the email that will contain the one-time password. (For more information about one-time passwords, see Using One-Time Passwords for Added Security.)
19. Click **Save**.

Testing AD,LDAP,RADIUS and One Defender Authentication Configurations

To help you validate your authentication configuration settings, the AMC pages used to configure Microsoft Active Directory, LDAP, RADIUS, and One Defender servers include a **Test** button. Clicking this button establishes a connection with your external user repository and provides status information.



If you have correctly configured the appliance, a message reading `Valid connection!` appears. If there is an error in the configuration settings, the message provides a description of the problem.

ⓘ **NOTE:** The test connection feature is intended only for testing whether the appliance can bind to an external directory. If you enter login credentials, the appliance will use them, but it will otherwise attempt to bind to the directory anonymously. Because it does not actually search the directory, testing a connection will not validate that your login credentials provide access to the configured domain.

Configuring Chained Authentication

For increased security, you can require users to authenticate to a single realm using two different authentication methods. For example, you could set up RADIUS or a digital certificate as the first authentication method, and LDAP or Active Directory as the second one. The local authentication store can be used as either the primary or secondary authentication server. You can require that the user names are the same on the primary and secondary authentication servers. To make the login experience for your users a one-step process you can configure AMC such that users see only one set of prompts.

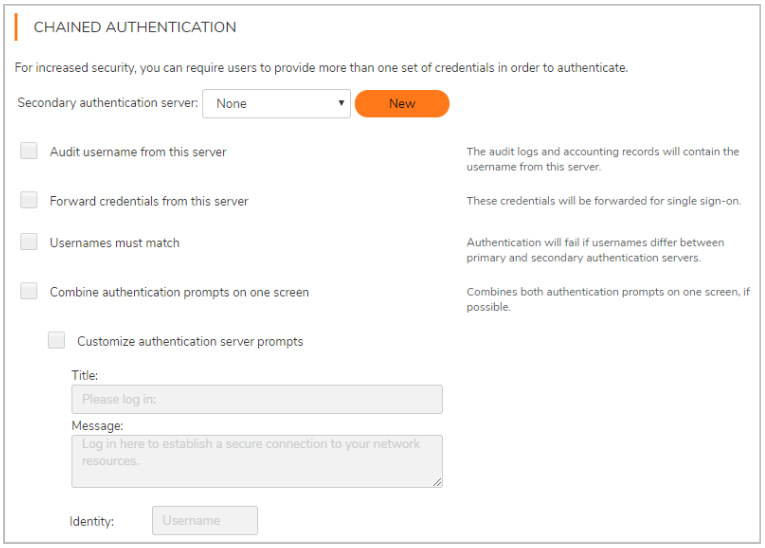
To configure chained authentication:

1. In the AMC, navigate to **User Access > Realms**.
2. Select the name of the realm you want to modify or click **New realm**.
3. In **General** tab enter the realm name and description for the users to select the realm.
   a. Select **Enabled** or **Disabled** to display the realm.
   b. Then select an entry in the **Authentication server** drop-down menu. For example, select RSA SecurID.

This is your primary authentication server.

If one of your credential types for chained authentication is a digital certificate, the corresponding authentication server must be the primary one: you can't configure a PKI server as your secondary authentication server.

4. Click **Advanced** and scroll to the **Chained authentication** section.



CHAINED AUTHENTICATION

For increased security, you can require users to provide more than one set of credentials in order to authenticate.

Secondary authentication server: None ▾ New

□ Audit username from this server	The audit logs and accounting records will contain the username from this server.
□ Forward credentials from this server	These credentials will be forwarded for single sign-on.
□ Usernames must match	Authentication will fail if usernames differ between primary and secondary authentication servers.
□ Combine authentication prompts on one screen	Combines both authentication prompts on one screen, if possible.

□ Customize authentication server prompts

Title: Please log in:

Message: Log in here to establish a secure connection to your network resources.

Identity: Username

a. Select a **Secondary authentication server** (if none is defined, click **New**; see Configuring Authentication Servers for the steps involved in setting up an authentication server). For example, select RSA SecurID.

b. The remaining (optional) settings, listed in the Authentication settings table, can provide more security, help with troubleshooting, and simplify the login process:

Authentication Settings

Setting	Description
Audit username from this server	Show the username from the secondary server in the audit and accounting logs (instead of the username from the primary authentication server).
Forward credentials from this server	For single sign-on, one set of credentials must be forwarded to back-end Web resources. Select this check box to forward the credentials from this (the secondary) authentication server. If RSA is configured as secondary authentication server, then this option is not available.

Usernames must match	When this check box is selected, authentication will fail if the user ID submitted for the first authentication step differs from the user ID submitted in the second step. This option is available when the authentication methods use either a username/password or a token or certificate. One use case for this option is when the primary authentication server uses a certificate and the secondary uses a username/password. Without this option enabled, an end user could log in with another user's certificate if the first user had valid credentials. When this setting is turned on, that authentication attempt would fail because the username in the certificate would not match the username in the username/password credentials.
Combine authentication prompts on one screen	When this check box is selected, the appliance verifies that the username is the same on both authentication servers. If it is, the prompts for a user's credentials are combined on a single screen; if the usernames differ, the login is rejected and (for security reasons) there is no error message explaining why. Authentication prompts cannot be combined if user credentials involve adigital certificate, though the system still ensures that the username is the same on both servers.
Customize authentication server prompts	(Available only when **Combine authentication prompts on one screen** is selected, and only for Windows clients.) When configuring an authentication server, you have the option of customizing the prompts that users see. When two such servers are chained together, you can present the user with a combined authentication prompt that includes customized **Title**, **Message**, and **Identity** fields. The name for the password fields is picked up from each authentication server configuration. If this customization setting is not selected, the user sees the prompts that are configured for the two authentication servers.

Refer to the section *Creating relams in SMA1000 Administration Guide* to complete the configurations and click **Finish**.

Chained Authentication Login Example

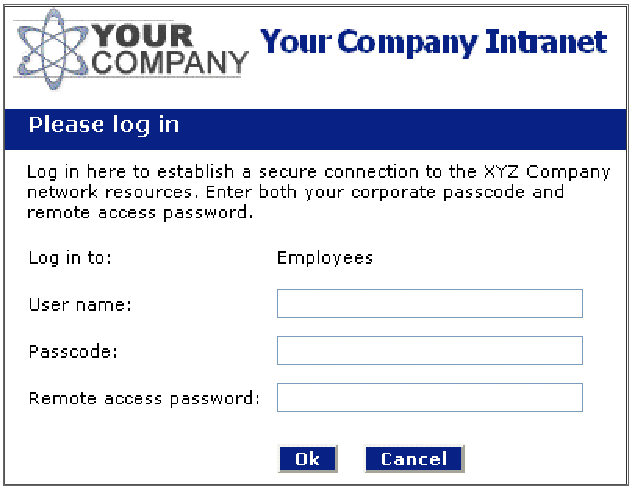
In this example, the system administrator has set up two authentication methods for a realm named *Employees*.

The primary authentication server uses RADIUS; the **Proof** prompt (on the **Configure Authentication Server** page, under **Advanced** settings) was customized to read *Passcode*.

The secondary authentication server uses LDAP; the **Proof** prompt was customized to read *Remote access password*.

The **Advanced** settings on the **Configure Realm - Employees** page show customized **Title**, **Message**, and **Identity** prompts.

Based on these AMC settings, the login screen that users see would look like this:



Please log in

Log in here to establish a secure connection to the XYZ Company network resources. Enter both your corporate passcode and remote access password.

Log in to: Employees

User name:

Passcode:

Remote access password:

Because the user names on both authentication servers are the same, the user types his or her username only once.

ⓘ | **NOTE:**

- If the user makes an error while entering username or password information, an error message appears (`The credentials provided were invalid`) and only the prompts for the secondary authentication server are displayed. To re-enter his or her credentials, the user must first go to the original login page by clicking the browser's **Back** button.
- When a username and password are used for both authentication methods, the usernames do not need to be the same (although they typically are). If the primary username is mapped to a role in AMC, such as the AMC Administrator Role, the secondary username does not need to be assigned to the same role. If authentication succeeds on both servers for both usernames, the user is granted access corresponding to the role of the primary username.

Enabling Group Affinity Checking in a Realm

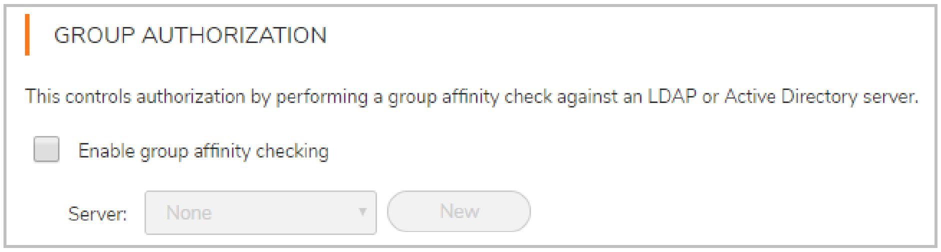
The appliance supports group affinity checking, a network environment in which a user authenticates against one server, and a second directory provides information on what groups (if any) a user belongs to. This is a common requirement when RADIUS SecurID tokens or SAML IdP are used for authentication but the user's group information comes from an LDAP or Active Directory server. (In contrast, chained authentication requires users to authenticate against two authentication servers. See Configuring Chained Authentication for more information).

Group membership is an important part of access control: you can set up the appliance to reference user groups stored in your directory, and then reference those groups in access control rules.

ⓘ | **NOTE:** When an Active Directory (AD) server is used as an LDAP server, ACL checks cannot be performed. Short names (SN) or common names (CN) are not supported on LDAP servers. They are only supported on AD servers.

To enable group affinity checking:

1. In the AMC, navigate to **User Access > Realms**.
2. Click the name of the realm you want to modify.
3. Click **Advanced**. In the **Group Authorization** area, select the **Enable group affinity checking** checkbox.



GROUP AUTHORIZATION

This controls authorization by performing a group affinity check against an LDAP or Active Directory server.

□ Enable group affinity checking

Server: None

4. In the **Server** drop-down menu, select the name of the LDAP or Active Directory server that stores the group information. You can also click **New** to define a new group affinity server.

   If group authorization checking is disabled for an authentication server, the server will not appear in the list of available affinity servers. See Disabling Authorization Checks for more information.
5. Click **Save**.

If you are enabling group affinity checking during the process of creating the realm, the available buttons are different:

- Click **Next** to display the **Communities** tab on the **Configure Realms** page.
- Click **Finish** to return to the **Authentication** page.

Using One-Time Passwords for Added Security

A one-time password (OTP) is a randomly generated password that is used only once. Using an OTP as the second factor for authentication provides additional security for users: after standard user name and password credentials are submitted, the system generates a one-time password, which is sent to the user at a predefined SMS or email address. The user then logs in to that email account to retrieve the OTP and enters it when prompted. The likelihood of the password being compromised is reduced because a new OTP is generated after each successful, canceled, or failed login, or when a login attempt has timed out.

SMA supports TOTP, SMS, and Email based one time passwords. For more details, refer to the Using Time-Based One-Time Passwords, Configuring SMTP to Deliver One-Time Passwordssections.

To configure authentication that includes an email-based OTP, you must do the following:

- Configure your mail server. If one-time passwords are going to be delivered to external domains (for example, an SMS address or external webmail address), you may have to configure the SMTP server to allow passwords to be sent from the appliance to the external domain.
- Configure an OTP in the **Advanced** area of the authentication server configuration. Specify the directory attributes that store the email addresses to which OTPs are sent.

You can also use Time-Based One-Time passwords (TOTP) that use third-party client applications for authentication. See Using Time-Based One-Time Passwords for more information.

Topics:

- Configuring SMTP to Deliver One-Time Passwords
- Configuring an Authentication Server for email-basedOne-Time Passwords
- Configuring Personal Device Authorization
- Using Time-Based One-Time Passwords
- Configuring the AD or LDAP Directory Server

Configuring SMTP to Deliver One-Time Passwords

If the email addresses to which you want to deliver one-time passwords are in an external domain (such as SMS addresses or external web mail addresses), you must configure your SMTP server to allow passwords to be sent from the appliance to the external domain.

To configure Microsoft Exchange to support one-time passwords:

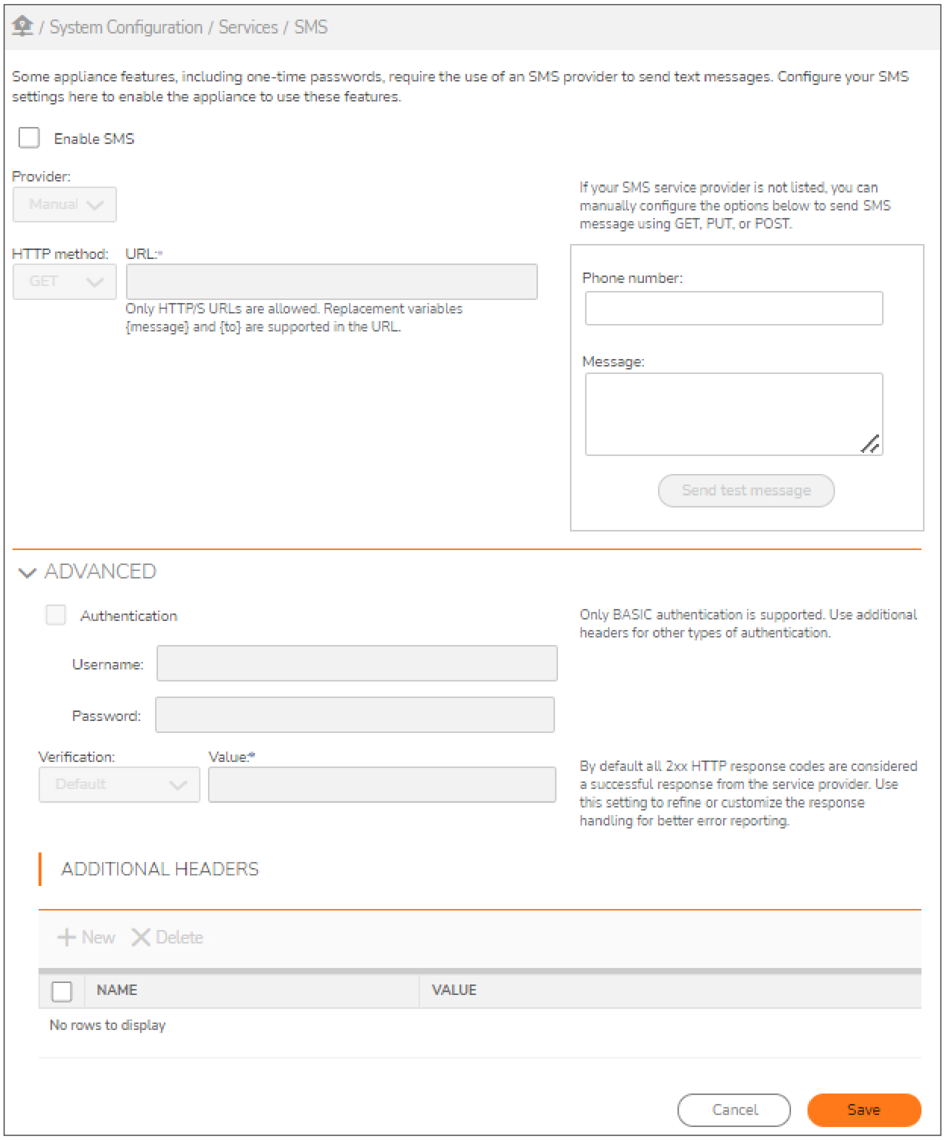
1. Navigate to **Exchange System Manager**.
2. Expand **Servers > Protocols > SMTP**.
3. Right-click on either **Default SMTP Virtual Server** or the appropriate SMTP server instance.
4. Click **Properties**.
5. Select the **Access** tab.
6. Click **Relay** in the **Relay Restrictions** area.
7. Select **Only the list below**.
8. Click **Add**.
9. Enter the IP address of your SMA appliance (for example, `10.50.165.5`).
10. Click **OK**.
    Your appliance should be listed with a status *Access Granted*.
11. Click **OK**.

Configuring SMS based Authentication

SMA allows OTP to be delivered through SMS along with the Email. SMS authentication is supported on Active Directory, AD-Advanced, LDAP, and Local Authentication servers. All the SMS Gateways that support HTTP/REST APIs are supported.

Configuring SMS Gateway

1. In the AMC, navigate to **System Configuration > Services > SMS > Configure**.



/ System Configuration / Services / SMS

Some appliance features, including one-time passwords, require the use of an SMS provider to send text messages. Configure your SMS settings here to enable the appliance to use these features.

□ Enable SMS

Provider: Manual

If your SMS service provider is not listed, you can manually configure the options below to send SMS message using GET, PUT, or POST.

HTTP method: GET

URL:*

Only HTTP/S URLs are allowed. Replacement variables {message} and {to} are supported in the URL.

Phone number:

Message:

ADVANCED

□ Authentication

Only BASIC authentication is supported. Use additional headers for other types of authentication.

Username:

Password:

Verification: Default

Value:*

By default all 2xx HTTP response codes are considered a successful response from the service provider. Use this setting to refine or customize the response handling for better error reporting.

ADDITIONAL HEADERS

□	NAME	VALUE

No rows to display

2. Click **Enable SMS**.

3. In the **Provider** drop-down, select the SMS gateway provider and provide account details.

> ⓘ **NOTE:** If your SMS service provider is not listed, you can manually configure the options by choosing **Manual** option from the Provider list. Refer the *HTTP/API/developer guide* provided by your SMS Gateway to configure manually.

Configuration Procedure

1. Select GET/POST/PUT method based on the Gateway API guide.

   GET method:

   a. Enter the URL endpoint to submit SMS

   b. In place of actual destination number, use the placeholder key {to}

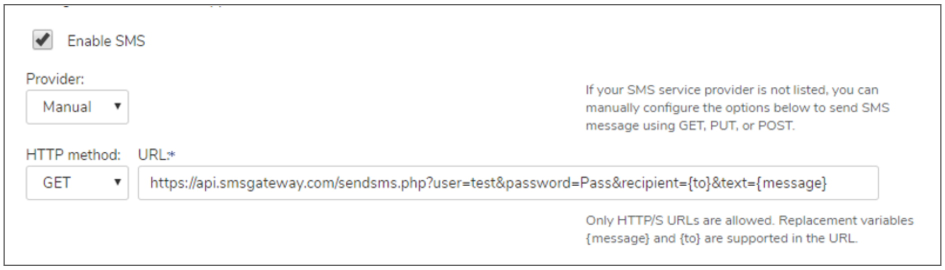
   c. In place of actual message, use the placeholder key {message}

      Example: If the URL endpoint provided by your gateway is:

      https://api.smsgateway.com/sendsms.php?user=test&password=Pass&recipient=33781723&text=This%20is%20a%20test%20message

      Configure it as

      https://api.smsgateway.com/sendsms.php?user=test&password=Pass&recipient={to}&text={message}



☑ Enable SMS

Provider: Manual ▾

If your SMS service provider is not listed, you can manually configure the options below to send SMS message using GET, PUT, or POST.

HTTP method: GET ▾

URL*: https://api.smsgateway.com/sendsms.php?user=test&password=Pass&recipient={to}&text={message}

Only HTTP/S URLs are allowed. Replacement variables {message} and {to} are supported in the URL.

POST/PUT method:

1. Enter the URL endpoint to submit SMS.
2. Select the Content type as Form/JSON/XML.
3. Enter the message to be shared.
4. In place of actual destination number, use the placeholder key {to}
5. In place of actual message, use the placeholder key {message}

   Example: If the URL endpoint provided by your gateway is

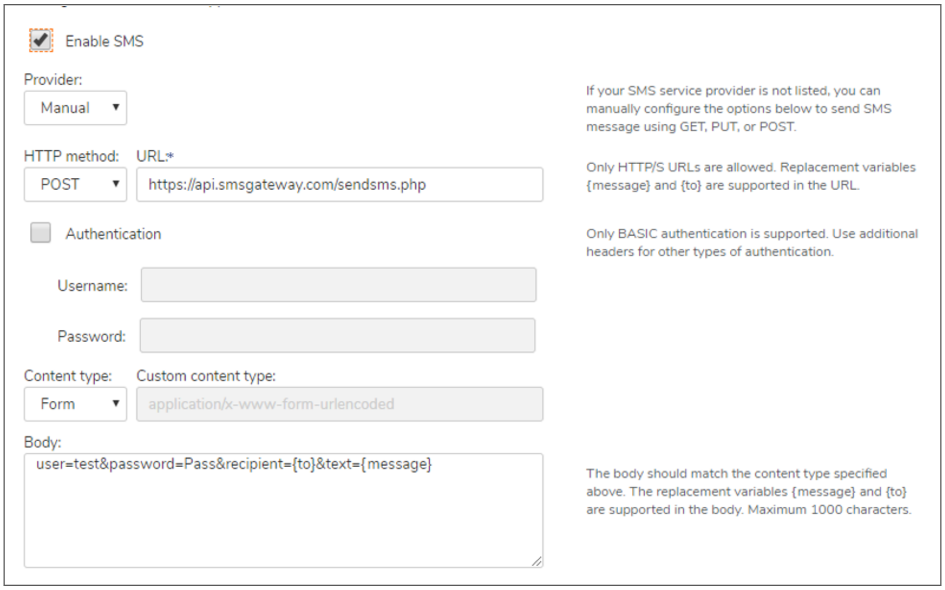
   https://api.smsgateway.com/sendsms.php

   with content type as application/x-www-form-urlencoded and body as user=test&password=Pass&recipient=33781723&text=This%20is%20a%20test%20message

   Configure it as:

   - Select POST/PUT method
   - Enter URL as https://api.smsgateway.com/sendsms.php
   - Select Content type as **Form**

- Enter Body as user=test&password=Pass&recipient={to}&text={message}



☑ Enable SMS

Provider: Manual

If your SMS service provider is not listed, you can manually configure the options below to send SMS message using GET, PUT, or POST.

HTTP method: POST

URL:* https://api.smsgateway.com/sendsms.php

Only HTTP/S URLs are allowed. Replacement variables {message} and {to} are supported in the URL.

□ Authentication

Only BASIC authentication is supported. Use additional headers for other types of authentication.

Username:

Password:

Content type: Form

Custom content type: application/x-www-form-urlencoded

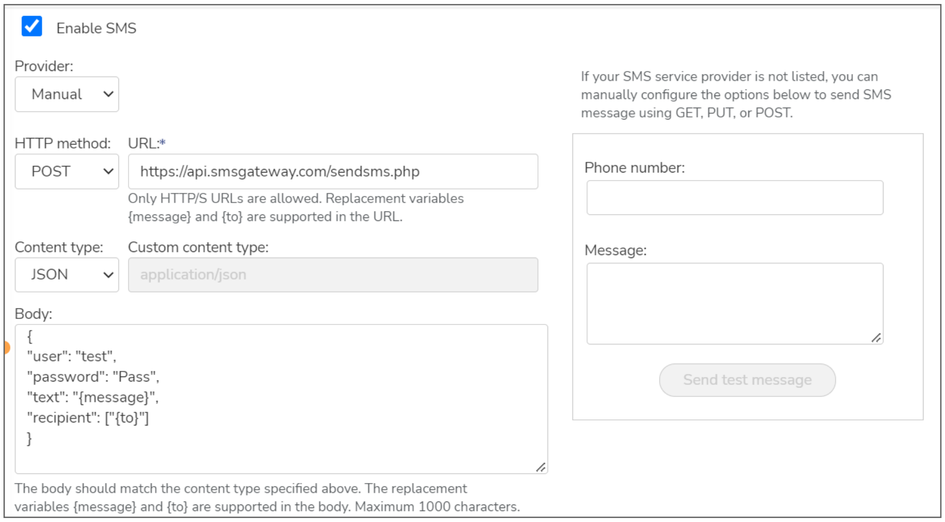
Body:

user=test&password=Pass&recipient={to}&text={message}

The body should match the content type specified above. The replacement variables {message} and {to} are supported in the body. Maximum 1000 characters.

6. In case of JSON content type, if original content to be sent is,

```
{
"user": "test",
"password": "Pass",
"text": "This is a test message",
"recipient": ["9239183"]
}
Provide replaced content as below
{
"user": "test",
"password": "Pass",
"text": "{message}",
"recipient": ["{to}"]
}
```



☑ Enable SMS

Provider: Manual

If your SMS service provider is not listed, you can manually configure the options below to send SMS message using GET, PUT, or POST.

HTTP method: POST

URL:* https://api.smsgateway.com/sendsms.php

Only HTTP/S URLs are allowed. Replacement variables {message} and {to} are supported in the URL.

Content type: JSON

Custom content type: application/json

Body:

```
{
"user": "test",
"password": "Pass",
"text": "{message}",
"recipient": ["{to}"]
}
```

The body should match the content type specified above. The replacement variables {message} and {to} are supported in the body. Maximum 1000 characters.

Phone number:

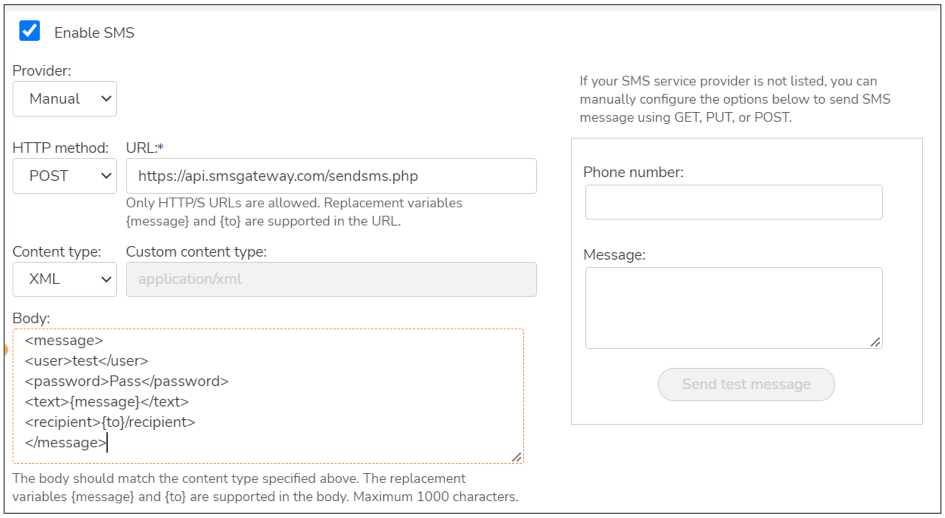
Message:

7. In case of XML content type, if original content to be sent is,

```
<message>
<user>test</user>
<password>Pass</password>
<text>This is a test message</text>
<recipient>9239183</recipient>
</message>
```

Provide replaced content as below:

```
<message>
<user>test</user>
<password>Pass</password>
<text>{message}</text>
<recipient>{to}/recipient>
</message>
```



☑ Enable SMS

Provider: Manual

If your SMS service provider is not listed, you can manually configure the options below to send SMS message using GET, PUT, or POST.

HTTP method: POST

URL:* https://api.smsgateway.com/sendsms.php

Only HTTP/S URLs are allowed. Replacement variables {message} and {to} are supported in the URL.

Content type: XML

Custom content type: application/xml

Body:

```
<message>
<user>test</user>
<password>Pass</password>
<text>{message}</text>
<recipient>{to}/recipient>
</message>
```

The body should match the content type specified above. The replacement variables {message} and {to} are supported in the body. Maximum 1000 characters.

Phone number:

Message:

2. Configure **Verification settings** to identify whether SMS gateway has accepted the message for submission. By default the HTTP status response code is considered for validation - all response status code between 200 and 299 is considered successful submission.

   To change this behavior:

   - Choose **Status code** and mention the specific status response code that should be considered as successful submission. All other response code from SMS Gateway will be considered as failure to submit SMS.
   - Choose **Contains text** option if your SMS gateway responds with specific response body on success. For Example, enter the text “OK”. If response body contains no instance of “OK”, it will be considered as failure to submit SMS.

3. In case your SMS Gateway expects account credentials over Basic HTTP authentication header, enable “Authentication” and provide the user details.

4. If SMS gateway expects account-id and password over HTTP header, use Additional headers option to add them.

5. To test the configuration:

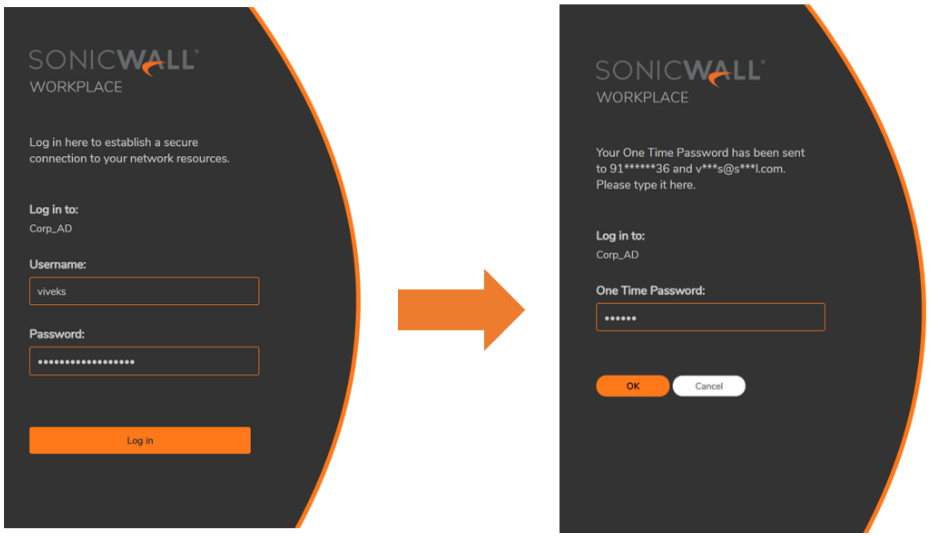
   a. In the **Phone number** field, enter the phone number to which the OTP needs to be delivered.

   b. In the **Message** field, type in the message. For example: Test message.

   c. Click **Send text message**.

      The text message is delivered to the entered phone number.

6. Click **Save**.



Log in here to establish a secure connection to your network resources.

Log in to: Corp_AD

Username: viveks

Password: ••••••••••••••••••

Your One Time Password has been sent to 91******36 and v***s@s***l.com. Please type it here.

Log in to: Corp_AD

One Time Password: ••••••

> **NOTE:** Once you have configured the SMS authentication, enable the SMS services in the authentication service to log in to the SMA using OTP. For more details, refer to the respective authentication server section in this guide.

Using Time-Based One-Time Passwords

The Time-Based One-Time Password (TOTP) is an alternative method of Two-Factor Authentication which can be more cost-effective when compared to traditional Two-Factor Authentication technologies. You can use client applications such as Google Authenticator and Microsoft Authenticator to generate the one-time passwords.

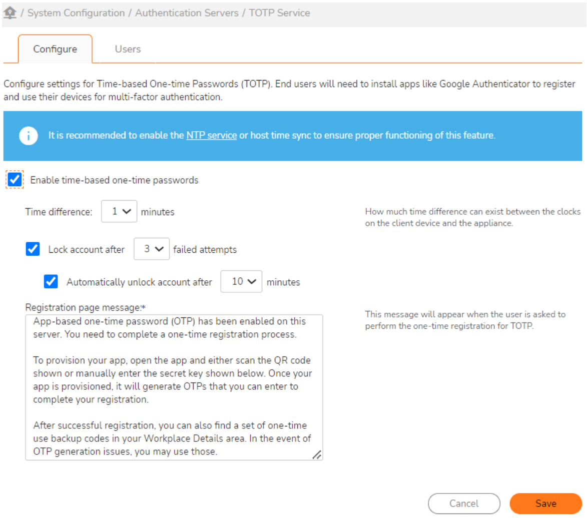
Topics:

- Configuring Time-Based One-Time Passwords Settings
- Managing Users of Time-Based One-Time Passwords

Configuring Time-Based One-Time Passwords Settings

To configure authentication servers to use time-based one-time passwords:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In the **Other Servers** section, click **Edit** next to **Configure time-based one-time password (TOTP) settings**.
3. Click **Configure**.



/ System Configuration / Authentication Servers / TOTP Service

Configure settings for Time-based One-time Passwords (TOTP). End users will need to install apps like Google Authenticator to register and use their devices for multi-factor authentication.

It is recommended to enable the NTP service or host time sync to ensure proper functioning of this feature.

☑ Enable time-based one-time passwords

Time difference: 1 minutes — How much time difference can exist between the clocks on the client device and the appliance.

☑ Lock account after 3 failed attempts

☑ Automatically unlock account after 10 minutes

Registration page message:*

App-based one-time password (OTP) has been enabled on this server. You need to complete a one-time registration process.

To provision your app, open the app and either scan the QR code shown or manually enter the secret key shown below. Once your app is provisioned, it will generate OTPs that you can enter to complete your registration.

After successful registration, you can also find a set of one-time use backup codes in your Workplace Details area. In the event of OTP generation issues, you may use those.

This message will appear when the user is asked to perform the one-time registration for TOTP.

4. Click **Enable time-based one-time passwords**.
5. Adjust the value in the **Time difference** field to adjust the time difference (in minutes) allowed between the clock on the client device and on the SMA appliance.
6. Set the value of the **Lock account after _ failed attempts** field to specify the number of unsuccessful attempts users can have before their account is locked. (This option is selected by default.)
7. Set the value of the **Automatically unlock account after _ minutes** field to specify the amount of time (in minutes) before user accounts will be automatically unlocked after being locked from too many unsuccessful login attempts. (This option is selected by default.)

   ⓘ **NOTE:** The user account is not automatically set to an unlocked state. It will be unlocked the next time that the user tries to log in, if the number of minutes specified in this field have passed since their last unsuccessful login attempt.

   If you do not want user accounts automatically unlocked, unselect this option.
8. Click **Save**.

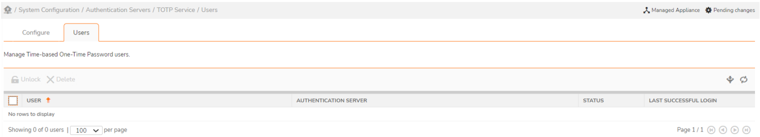
ⓘ **NOTE:** When you enable the usage of Time-Based One-Time Passwords, it is recommended that you only allow end users to register their devices through the WorkPlace or Connect Tunnel applications.

Managing Users of Time-Based One-Time Passwords

To manage users of time-based one-time passwords:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In the **Other servers** section, click **Edit** next to **Configure time-based one-time password (TOTP) settings**.

3. Click the **Users** tab.



/ System Configuration / Authentication Servers / TOTP Service / Users

Manage Time-based One-Time Password users.

□	USER	AUTHENTICATION SERVER	STATUS	LAST SUCCESSFUL LOGIN
	No rows to display			

Showing 0 of 0 users | 100 per page

Page 1 / 1

To unlock time-based one-time password user accounts:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In the **Other servers** section, click **Edit** next to **Configure time-based one-time password (TOTP) settings**.
3. Click **Users**.
4. Select the user accounts you want to unlock in the list.
5. Click the **Unlock** icon.

To delete time-based one-time password user accounts:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In the **Other servers** section, click **Edit** next to **Configure time-based one-time password (TOTP) settings**.
3. Click **Users**.
4. Select the user accounts you want to delete in the list.
5. Click the **Delete (X)** icon.

After you have deleted a user account, the user will be prompted again to receive a new time-based one-time password and backup codes.

> ⓘ **NOTE:** To allow users to deregister their account themselves, enable **Allow user to deregister account** option under One-Time Passwords section of Authentication server. This will provide an option on WorkPlace for user to deregister their account. Once deregistered, user will be prompted to register a new account during next login.

Configuring an Authentication Server for email-basedOne-Time Passwords

If the email addresses to which you want to deliver one-time passwords are in an external domain (such as SMS addresses or external web mail addresses), you must configure your SMTP server to allow passwords to be sent from the appliance to the external domain, as described in Configuring SMTP to Deliver One-Time Passwords.

For each authentication server, you must also specify the directory attribute that stores the email addresses to which OTPs are sent. You must specify a primary attribute; alternatively, you can specify a secondary attribute that is queried when the first one cannot be found.

To configure an authentication server to support one-time passwords:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. Click **Edit** next to the AD (**Microsoft Active Directory Basic or Microsoft Active Directory Advanced**), LDAP, or local authentication server you want to reconfigure.
3. Select a **Credential type**, if applicable.
4. Click **Continue**.
5. Expand the **Advanced** area,
6. Scroll down to the **One-Time Passwords** section and select **Use one-time passwords with this authentication server**.
7. Enter the directory attribute for the email address to which one-time passwords will be sent. If the primary attribute exists on the authentication server, it is used, otherwise the secondary attribute, if specified, is queried.

Configuring the AD or LDAP Directory Server

The schema for your AD or LDAP directory server must include an attribute that contains the email address to which a one-time password will be sent. The local authentication store uses the **primaryEmail** attribute, which can be configured per user by editing the local user account. See Managing Local User Accounts.

This address is not necessarily the user's corporate email address. In order to complete authentication, a user has to be able to open the email containing the OTP; if it is sent to a corporate address the user may not yet have access to the account.

One-time passwords can be configured to be sent in an email message directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS.

The schema for your directory server (AD or LDAP) must be changed to accommodate an attribute (for example, **SMSphone**) that contains the SMS address for a given user. The address that you use depends on the user's number and service provider. The attribute value for a Verizon phone with a U.S. domestic number, for example, looks like this: `<10-digit number>@vtext.com`.

Configuring Personal Device Authorization

With Personal Device Authorization users connecting to the corporate network with a personal device that is not registered with the appliance are prompted to register the device. They must agree to the personal device corporate policies and privacy policies to access corporate resources.

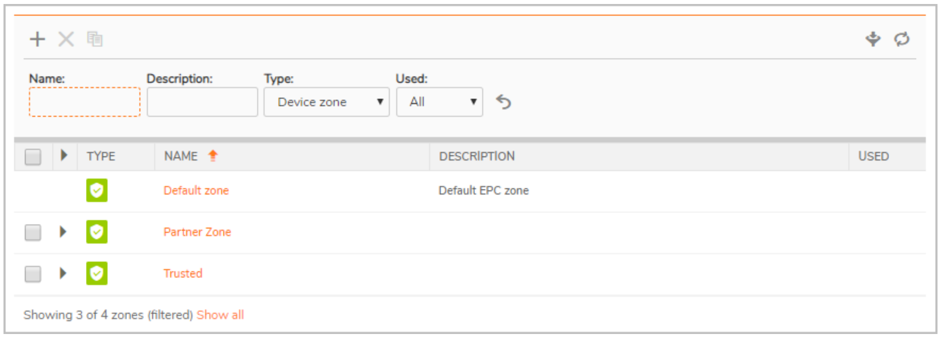
After the user consents to the corporate policies for a device, the device's unique Device ID is determined and the appliance registers the device to the user. Subsequent connections from this device do not require device authorization.

In addition, you can monitor usage of personal devices that have accessed the appliance, as explained in Viewing User Access and Policy Details

__To create an Device Zone for Personal Device Authorization:__

1. Navigate to **User Access > End Point Control** page
2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.
3. Select **Device zone** from the **Filters Type** drop-down menu, and then click the **Refresh** icon.

   All device zones are displayed.



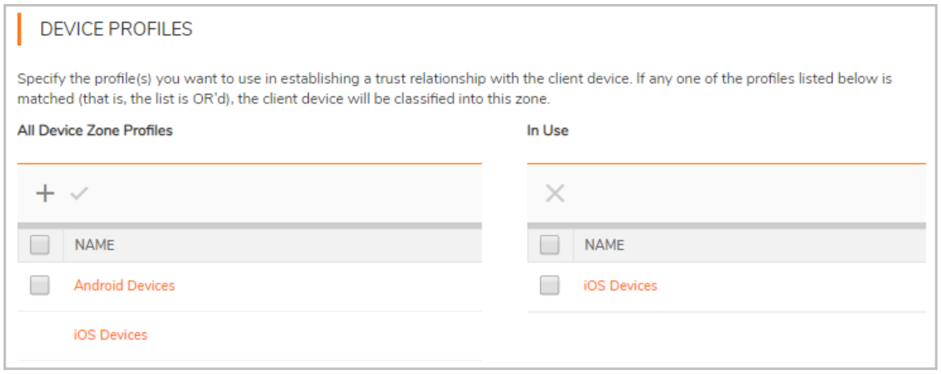
Name: | Description: | Type: Device zone | Used: All

	TYPE	NAME	DESCRIPTION	USED
	✓	Default zone	Default EPC zone	
□	✓	Partner Zone		
□	✓	Trusted		

Showing 3 of 4 zones (filtered) Show all

4. Click on any zone to display **Device profiles**.

   Only those profiles that are Application Access Control aware are included in the profiles.



DEVICE PROFILES

Specify the profile(s) you want to use in establishing a trust relationship with the client device. If any one of the profiles listed below is matched (that is, the list is OR'd), the client device will be classified into this zone.

All Device Zone Profiles

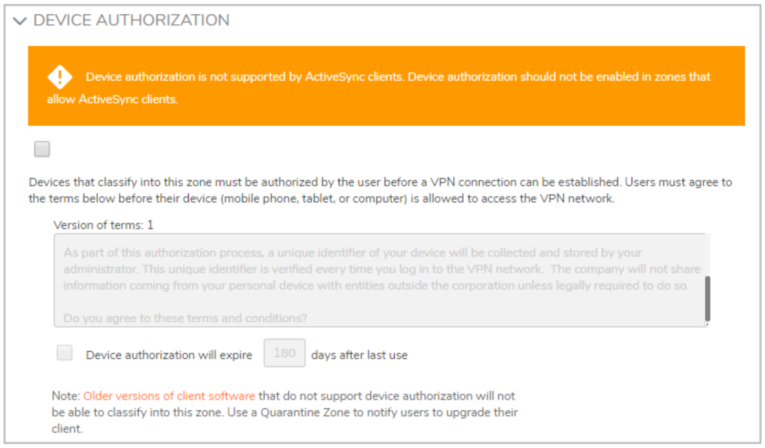
□	NAME
□	Android Devices
	iOS Devices

In Use

□	NAME
□	iOS Devices

5. In the **All Device Zone Profiles** list, select the checkbox for any profiles that you want to require in the zone.
6. Click the right arrow (**>>**) button. Only one of the profiles in the **In Use** list needs to match for the application to be placed in the zone you are creating.

   If there are no device profiles for this zone, click **New** to add one.
7. Expand **Device authorization**.



DEVICE AUTHORIZATION

Device authorization is not supported by ActiveSync clients. Device authorization should not be enabled in zones that allow ActiveSync clients.

□

Devices that classify into this zone must be authorized by the user before a VPN connection can be established. Users must agree to the terms below before their device (mobile phone, tablet, or computer) is allowed to access the VPN network.

Version of terms: 1

As part of this authorization process, a unique identifier of your device will be collected and stored by your administrator. This unique identifier is verified every time you log in to the VPN network. The company will not share information coming from your personal device with entities outside the corporation unless legally required to do so.

Do you agree to these terms and conditions?

□ Device authorization will expire 180 days after last use

Note: Older versions of client software that do not support device authorization will not be able to classify into this zone. Use a Quarantine Zone to notify users to upgrade their client.

8. Check the top checkbox in the **Device Authorization** area to require users to authorize their personal device before a VPN connection is established.
9. To change the authorization terms that users must agree to, type the desired authorization terms in the **Terms** section of the **Device Authorization** area. The **Device Authorization** checkbox must be checked to edit the terms.
10. By default, a user authorization expires **180** days after the device was last used. When device authorization is enabled, you can disable zone authorization expiration by unchecking the expiration checkbox or change the number of days before expiration by typing the desired number of days.
11. By default, user connections to a zone are not dropped when the connection is inactive. However, a inactivity timer can be set In the **Inactivity timer** area to end the connection after a set period of inactivity. The inactivity timer interval can be set from 3 minutes to 10 hours.
12. Add the zone to a community as explained in Using End Point Control Restrictions in a Community.

Using Your SMA Appliance as a SAML Identity Provider

With Secure Mobile Access 12.4, your SMA appliance can become an on-box SAML Identity Provider (IdP), improving security for customers using cloud-based applications such as Salesforce or Office365.

The Secure Mobile Access appliance can:

- Behave as an Identity Provider
- Support web browser SSO profiles
- Support HTTP POST/Redirect Binding for SAML requests

A SAML IdP provides user information (after authentication) to other applications using the SAML protocol. These applications can be configured to trust an Identity Provider for the authentication of their users. After the IdP has authenticated users' credentials, it will redirect the users to the application, passing along any required user attributes, such as an email address or user name. Having your applications configured to trust an IdP can eliminate the need for users to login into each of the applications individually when they access them.

SAML authentication is supported on Tunnel clients (Connect Tunnel, and Mobile Connect Tunnel). Enable the clients to authenticate against third party SAML IdP servers. For more details, refer respective *Connect Tunnel Client User Guide*.

You can also configure external SAML Service Providers as resources. You should configure each service provider as a separate SAML Service Provider resource. See Adding Resources for more information.

Support for User Groups in SAML IdP Authentication

SMA and CMS is enhanced to support SAML authentication for Administrators. Also, SMA is enhanced to support group membership details over SAML authentication and users without on-premise Active Directory can now have group level management.

ⓘ **NOTE:** Prior to SMA 12.4.1 version, group membership details of users are not available to SMA when using SAML IdP authentication.

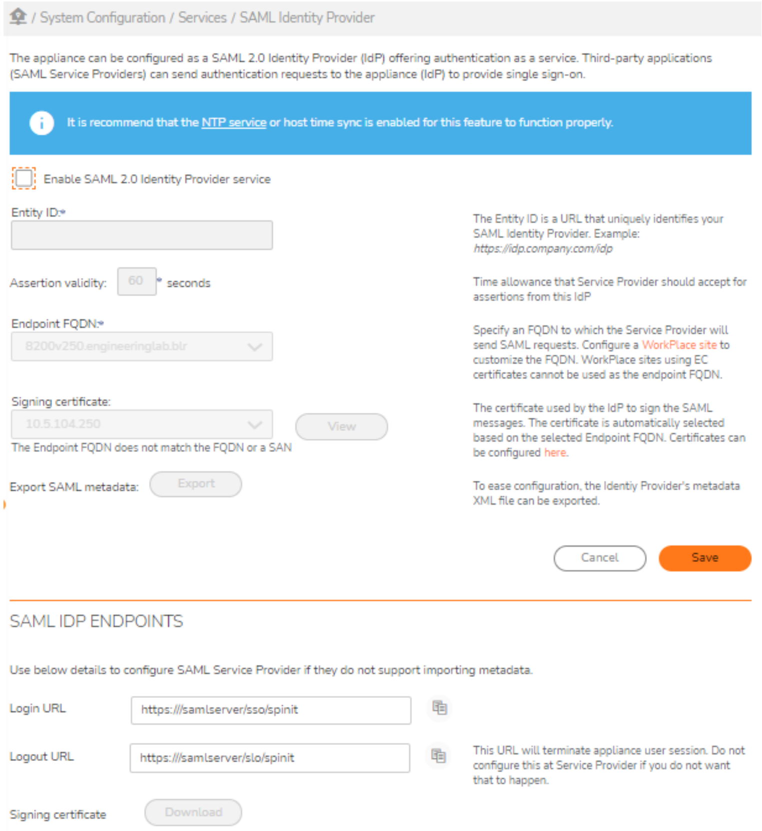
For more information on how to configure user group support in SAML authentication, see Configuring a SAML 2.0 Identity Provider Authentication Server.

Configuring Your SMA Appliance to be a SAML IdP

For your SMA appliance to operate as an Identity Provider, trust needs to be established between the application and your SMA appliance.

To configure your SMA appliance to be SAML IdP:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **SAML Identity Provider**, click **Configure**.



/ System Configuration / Services / SAML Identity Provider

The appliance can be configured as a SAML 2.0 Identity Provider (IdP) offering authentication as a service. Third-party applications (SAML Service Providers) can send authentication requests to the appliance (IdP) to provide single sign-on.

It is recommend that the NTP service or host time sync is enabled for this feature to function properly.

□ Enable SAML 2.0 Identity Provider service

Entity ID:*

The Entity ID is a URL that uniquely identifies your SAML Identity Provider. Example: *https://idp.company.com/idp*

Assertion validity: 60 * seconds

Time allowance that Service Provider should accept for assertions from this IdP

Endpoint FQDN:* 8200v250.engineeringlab.blr

Specify an FQDN to which the Service Provider will send SAML requests. Configure a WorkPlace site to customize the FQDN. WorkPlace sites using EC certificates cannot be used as the endpoint FQDN.

Signing certificate: 10.5.104.250

The Endpoint FQDN does not match the FQDN or a SAN

The certificate used by the IdP to sign the SAML messages. The certificate is automatically selected based on the selected Endpoint FQDN. Certificates can be configured here.

Export SAML metadata:

To ease configuration, the Identiy Provider's metadata XML file can be exported.

SAML IDP ENDPOINTS

Use below details to configure SAML Service Provider if they do not support importing metadata.

Login URL https:///samlserver/sso/spinit

Logout URL https:///samlserver/slo/spinit

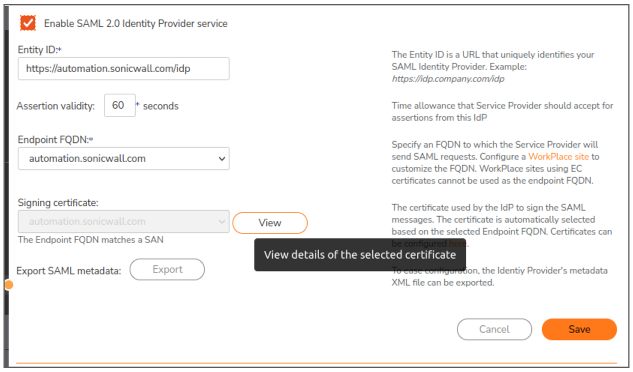
This URL will terminate appliance user session. Do not configure this at Service Provider if you do not want that to happen.

Signing certificate

3. Select **Enable SAML 2.0 Identity Provider service** to enable the SMA appliance as an Identity Provider.
4. In the **Entity ID** field, enter the URL that uniquely identifies your SAML Identity Provider. For example, ***https://idp.company.com/idp***.
5. Set the value in the **Assertion validity** field for the time allowance (in seconds) that the application should accept for assertions from your SMA appliance.
6. In the **Endpoint FQDN** field, specify an FQDN to which the application will send SAML requests.

   ⓘ | **NOTE:** You will need to configure a WorkPlace site in order to customize the FQDN.

   The **Signing certificate** field displays the location of the certificate used by the IdP to sign its SAML messages. The certificate is automatically selected based on the **Endpoint FQDN**. (You can configure certificates in the **SSL Settings > General** page. For more information, see Certificates).



☑ Enable SAML 2.0 Identity Provider service

Entity ID:* https://automation.sonicwall.com/idp

The Entity ID is a URL that uniquely identifies your SAML Identity Provider. Example: *https://idp.company.com/idp*

Assertion validity: 60 * seconds

Time allowance that Service Provider should accept for assertions from this IdP

Endpoint FQDN:* automation.sonicwall.com

Specify an FQDN to which the Service Provider will send SAML requests. Configure a WorkPlace site to customize the FQDN. WorkPlace sites using EC certificates cannot be used as the endpoint FQDN.

Signing certificate: automation.sonicwall.com

The Endpoint FQDN matches a SAN

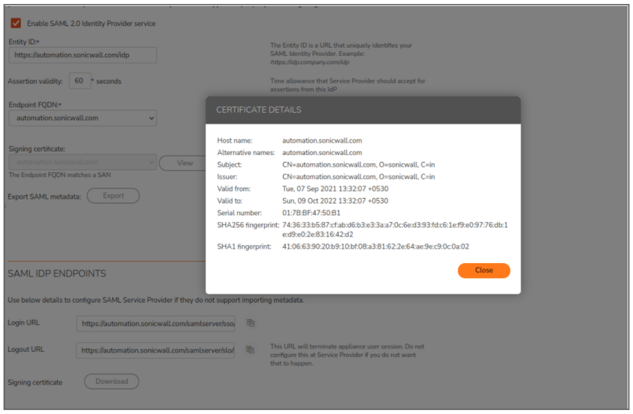
The certificate used by the IdP to sign the SAML messages. The certificate is automatically selected based on the selected Endpoint FQDN. Certificates can be configured here.

View details of the selected certificate

Export SAML metadata:

To ease configuration, the Identiy Provider's metadata XML file can be exported.

a. Click the **View** button to view the signing certificate.

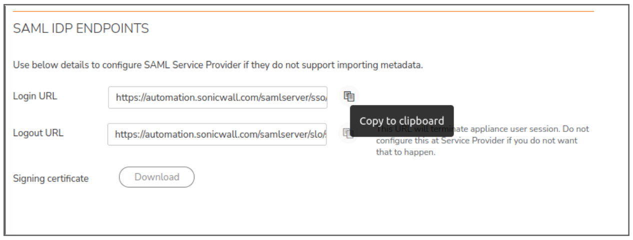


CERTIFICATE DETAILS

Host name:	automation.sonicwall.com
Alternative names:	automation.sonicwall.com
Subject:	CN=automation.sonicwall.com, O=sonicwall, C=in
Issuer:	CN=automation.sonicwall.com, O=sonicwall, C=in
Valid from:	Tue, 07 Sep 2021 13:32:07 +0530
Valid to:	Sun, 09 Oct 2022 13:32:07 +0530
Serial number:	01:7B:BF:47:50:B1
SHA256 fingerprint:	74:36:33:b5:87:cf:ab:d6:b3:e3:3a:a7:0c:6e:d3:93:fd:c6:1e:f9:e0:97:76:db:1e:d9:e0:2e:83:16:42:d2
SHA1 fingerprint:	41:06:63:90:20:b9:10:bf:08:a3:81:62:2e:64:ae:9e:c9:0c:0a:02

b. Click **Close**.

7. Under **SAML IdP Endpoint** section, the **Login URL** and **Logout URL** is displayed.



SAML IDP ENDPOINTS

Use below details to configure SAML Service Provider if they do not support importing metadata.

Login URL https://automation.sonicwall.com/samlserver/sso/

Logout URL https://automation.sonicwall.com/samlserver/slo/

This URL will terminate appliance user session. Do not configure this at Service Provider if you do not want that to happen.

Signing certificate

a. Click ⧉ to copy the URLs.

b. Click **Download**

8. Click the **Export** button to export the SAML metadata to an XML file that can be imported when configuring applications to accept your SMA appliance as an Identity Provider.

9. Click **Save**.

Biometric Identification

Topics:

About Biometric Identification

This feature provides the option to use biometric identification to unlock cached credentials on Mobile Connect devices.

Credential caching allows the user to establish a connection to the SMA appliance without having to reenter authentication credentials. Credential caching provides convenience, but it could allow an unauthorized user to access a corporate network if the user device is used by someone other than the owner. Biometric identification can be used to control who can access these cached credentials.

With biometric identification, a user can use a face or fingerprint to unlock their cached credentials.

Administrators can enable biometric identification on iOS devices and Android devices. End users can choose to require biometric identification in addition to their cached credentials for authentication.

Administrators can:

- Choose to enable credential caching.
- Choose to allow certain types of clients (iOS, Android, or both) to use credential caching.
- Choose to allow credential caching only in conjunction with biometric identification.

You can prevent any user from using another person's biometric identification to access a corporate network by disabling biometric identification for that user in their configuration settings. We recommend that you include a *Terms-of-Use* statement that states that a device using biometrics to unlock cached credentials only contains biometric signatures for the individual whose credentials are cached. With this feature, you can only use biometric identification to unlock cached credentials, and then use the cached credentials for authentication.

ⓘ **NOTE:** Biometric Identification is not supported with the Connect Tunnel client or web access methods (Mobile Connect only).

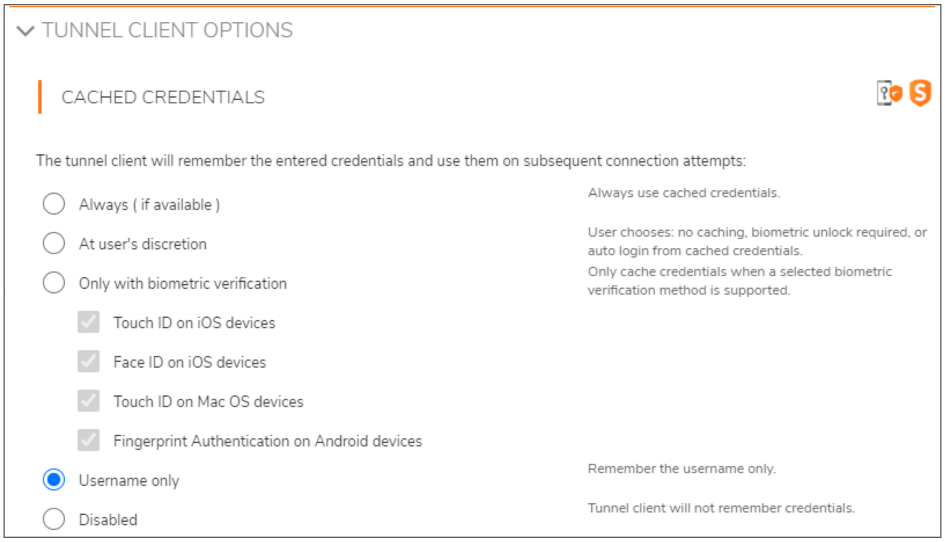
Configuring Biometric Identification

You can configure biometric identification using the SMA user interface.

To enable Allow Biometric ID:

1. In the AMC, navigate to **User Access > Realms**.
2. Click on the **Community** element for the realm you want to configure.
3. Select the **Tunnel Access** option.

4. Expand the **Tunnel client options** section.



TUNNEL CLIENT OPTIONS

CACHED CREDENTIALS

The tunnel client will remember the entered credentials and use them on subsequent connection attempts:

○ Always (if available) — Always use cached credentials.

○ At user's discretion — User chooses: no caching, biometric unlock required, or auto login from cached credentials.

○ Only with biometric verification — Only cache credentials when a selected biometric verification method is supported.

- ☑ Touch ID on iOS devices
- ☑ Face ID on iOS devices
- ☑ Touch ID on Mac OS devices
- ☑ Fingerprint Authentication on Android devices

● Username only — Remember the username only.

○ Disabled — Tunnel client will not remember credentials.

5. Navigate to the **Cached Credentials** section and select one of these options:

Option	Description
Always (if available)	Always use cached credentials
At user's discretion	Choose no caching, biometric unlock required, or auto login from cache.
Only with biometric verification	Only use credential caching when biometric verification is supported and enabled. Cached credentials are only used after biometric identification verification.
Username only	Use cached username.
Disabled	Disable cached credentials in the Connect Tunnel client.

6. If you selected **Only with biometric verification**, choose at least one of these options:

   - **Touch ID on iOS devices**
   - **Face ID on iOS devices**

     ⓘ **NOTE:** Face ID is currently only supported on iPhone X onwards. Support for Face ID in SMA requires Mobile Connect 5.0.2 (5031) or later, and is not supported by Connect Tunnel.

   - **Touch ID on Mac OS devices**
   - **Fingerprint Authentication on Android devices**

Next Steps

After you have performed the basic network setup, obtained an SSL certificate for the appliance, and configured authentication settings, you are ready to start managing users and user groups, defining resources, and configuring access control rules.

5

Administration

Topics:

- Security Administration
- System Administration

Security Administration

Topics:

- Creating and Managing Resources
- Access Control Rules

Creating and Managing Resources

Managing security is perhaps your most important job as an administrator. The Appliance Management Console (AMC) makes it easy for you to manage the fundamental elements of security administration: resources and access control rules.

This section explains how to create and manage individual resources, resource groups, and configuration settings for resources. You can define a resource before referencing it in an access control rule, or define it directly from the access control rule interface. (For more information about the latter, see Adding Users and Resources From Within Access Control Rules).

Topics:

- Resource Types
- Resources and Resource Groups
- Using Variables in Resource and WorkPlace Shortcut Definitions
- Creating and Managing Resource Groups
- Web Application Profiles
- Creating Forms-Based Dynamic Single Sign-On Profiles
- Kerberos Constrained Delegation
- Configuring SMA Support for Microsoft Outlook Anywhere

Resource Types

The SMA appliance provides access to a wide variety of corporate resources, which fall into these categories:

- Built-In Resources
- Web Resources
- Client/Server Resources
- File Share Resources

Built-In Resources

There are several resources that are built into your appliance to help you get a WorkPlace portal set up quickly. These built-in resources cannot be deleted—access to some of them is granted through WorkPlace shortcuts.

Topics:

- Secure Mobile Access WorkPlace (Resource Type: URL)
- Connect Tunnel (Resource Type: URL)
- Network Explorer (Resource Type: Network Share)

Secure Mobile Access WorkPlace (Resource Type: URL)

The WorkPlace portal gives users access to Web-based resources. This particular resource is used by another built-in item, which you can modify: an access permit-all rule that allows any user from any zone to have access to the default WorkPlace portal.

Value:`http://127.0.0.1:8085/workplace/`

Connect Tunnel (Resource Type: URL)

Connect Tunnel is an application that provides broad access to network resources. You determine how users access the Connect Tunnel client:

- Allow users to download the Connect Tunnel client and activate it from a link (shortcut) in WorkPlace. Keep in mind that when you give users access to this resource, you allow them to both install and use the client: a user without access to this resource cannot use Connect Tunnel for access to network resources. The WorkPlace shortcut for this resource (*Install Connect Tunnel*) can be modified or deleted; the resource itself cannot.
- Deploy the Connect Tunnel client setup package without requiring users to log in to Secure Mobile Access WorkPlace.

Value: `http://127.0.0.1:8085/ctdownload/`

Network Explorer (Resource Type: Network Share)

Network Explorer is a Web-based extension, accessible from WorkPlace, that provides access to any Windows file system resources that the user has permission to use (even from desktop browsers on non-Windows platforms). These resources can include servers, computers, workgroups, folders, and files. The WorkPlace shortcut for this resource (Network Explorer) can be modified or deleted; the resource itself cannot.

Value: `smb://127.0.0.1/networkexplorer/`

ⓘ **NOTE:** cTo set the maximum protocol level published by smb client when negotiating with server, use CEM `SMB_CLIENT_MAX_PROTOCOL`

For Example: `SMB_CLIENT_MAX_PROTOCOL = SMB2`

Web Resources

Web resources include Web-based applications or services that are accessed using HTTP or HTTPS. Examples include Microsoft Outlook Web Access and other Web-based email programs, Web portals, corporate intranets, and standard Web servers.

Web traffic is proxied through the Web proxy service, a secure gateway through which users can access private Web resources from the Internet. When you define a Web resource as a destination in an access control rule, make sure that **Web browser** is among the client software agents available for the rule. For more information, see Resolving Invalid Destination Resources.

A Web resource can be defined in various ways, as shown in the below table.

Web Resource Example Definitions

URL Type	Example
Standard URL	`http://host.example.com/index.html`
Standard URL with port number	`http://host.example.com:8445/index.html`
URL for secure site	`https://host.example.com/index.html`
URL containing IP address	`http://192.0.34.0/index.html`

Matching URL	Use wildcards to refer to a group of Web resources: `http://mailserver*.company.com/` **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.
URL with path and query string matching	Block email attachments, or prevent a Web-based application from displaying restricted data by matching a path element or query string value to a particular URL: `http://www.patient-records.com/reports.aspx?last_name=`

> **NOTE:** Some Web-based applications use JavaScript or other browser extensions using protocols other than HTTP. Although these applications are accessed using a Web browser, they must be defined as client/server (not Web resources), and they must be accessed using either a network tunnel client or client/server proxy agent. Examples of such applications include Oracle J-Initiator, and certain versions of SAP and PeopleSoft.

Client/Server Resources

Client/server resources are enterprise applications that run over TCP/IP (including applications that use UDP). Examples include thin-client applications such as Citrix; full client/server applications such as Microsoft Outlook; Lotus Notes; SAP; and terminal servers.

You define these types of client/server applications by specifying a host name, an IP address or IP range, a subnet IP address, or a DNS domain. These resources can also be used to define a network object containing multiple Web resources (such as a domain), or to define a network object that can be used to control access based on the source of a connection request.

The below table explains the syntax used to define each of these resource types. Host names can be fully qualified or unqualified.

Resource Type Syntax

Resource type	Example
Domain	`private.example.com`
Host name	`bart.private.example.com`
Host IP address	`192.0.34.72`
IP range	`192.0.34.72 - 192.0.34.74`
Subnet	`192.0.34.0 / 255.255.255.0`

Example

In this example, a Web development team has a single Web server with three virtual Web servers, one for each stage in their development process. Each virtual Web server listens on a different port.

Rather than creating three different URL resources, the Web development team can define the Web server, which proxies traffic on all ports, as a resource type of **Host name or IP** (for example, `webdev.yourcompany.com`). In addition, they attach a single sign-on Web application profile to it, and now all three of the virtual Web servers are defined at once, and they share the same SSO profile:

```
webdev.yourcompany.com

webdev.yourcompany.com:8080

webdev.yourcompany.com:8443
```

ⓘ **NOTE:** Microsoft Outlook connects to Microsoft Exchange using an unqualified host name. When defining a Microsoft Exchange server as a resource, define it as an unqualified name (for example, CorpMail).

To use Exchange on Android or iOS devices, create a URL resource of the type ActiveSync for Exchange.

File Share Resources

When users log in to WorkPlace, they have access to file system resources that you set up. These can include computers containing shared folders and files and Windows network servers.

You can define a specific file system share by typing a UNC path, or you can define an entire Windows domain:

- A specific file system resource can be an entire server (for example,`\\ginkgo`), a shared folder (`\\john\public`), or a network folder (`\\ginkgo\news`).
- Defining an entire Windows domain gives authorized users access to all the network file resources within the domain. These resources are the same ones you would see if you were to browse the network using Windows Explorer (**My Network Places > Entire Network > Microsoft Windows Network**).

You can use resource variables to dynamically reference multiple folders on the network. For example, to give each user access to a personal folder, create a resource using a variable for the user name, and then use that variable when you create a shortcut on WorkPlace. See the example in Using Session Property Variables for more information.

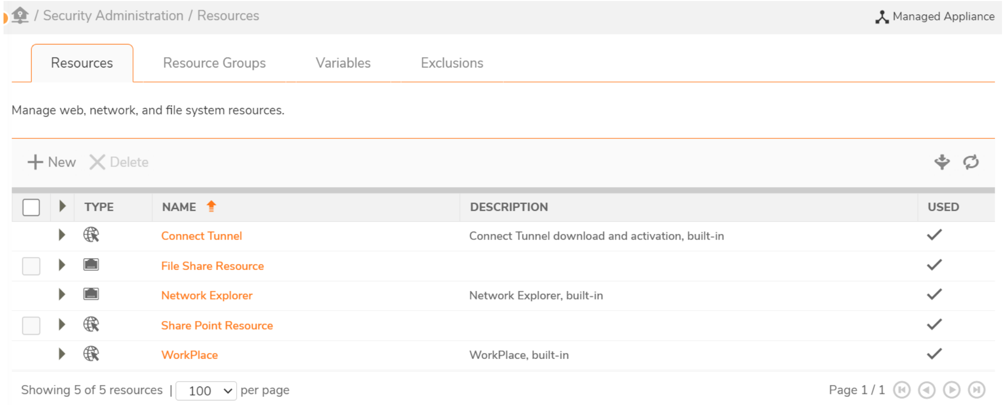
Resources and Resource Groups

Topics:

- Viewing Resources and Resource Groups
- Adding Resources
- Example: Specifying a URL Alias
- Example: Blocking Email Attachments
- Example: Supporting Exchange on iPhones
- Example: Restricting Access to Sensitive Data
- Editing Resources
- Deleting Resources
- Using the Exclusions

Viewing Resources and Resource Groups

You can view and define individual resources or groups of them in AMC on the **Security Administration > Resources** page.



Manage web, network, and file system resources.

☐		TYPE	NAME	DESCRIPTION	USED
	▸		Connect Tunnel	Connect Tunnel download and activation, built-in	✓
☐	▸		File Share Resource		✓
	▸		Network Explorer	Network Explorer, built-in	✓
☐	▸		Share Point Resource		✓
	▸		WorkPlace	WorkPlace, built-in	✓

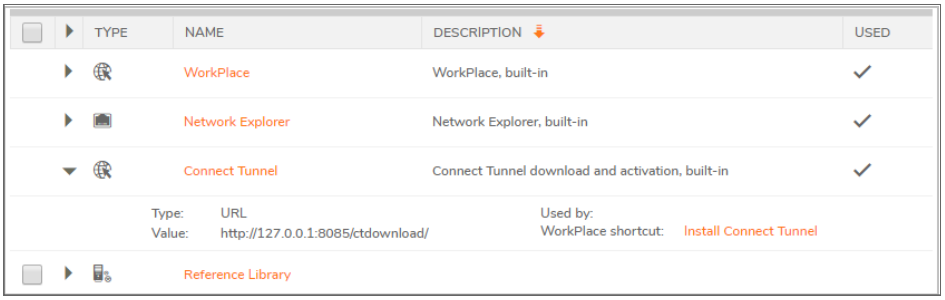
Showing 5 of 5 resources | 100 per page

Page 1 / 1

To view the list of available resources and resource groups:

1. In the AMC, navigate to **Security Administration > Resources**.
2. On the **Resources** tab, review the list of available individual resources. (The **Resource Groups** tab displays collections of resources.)
3. Click the **Filters** icon at the top right of the table to filter the resources that are displayed here. For information about using filters, see Filters:
    - The **Type** column displays the type of each resource (such as **Domain name**, **Host name**). Remember that a client/server resource can contain both Web and client/server applications.
    - The **Used** column indicates whether a resource has been specified in a shortcut on WorkPlace.

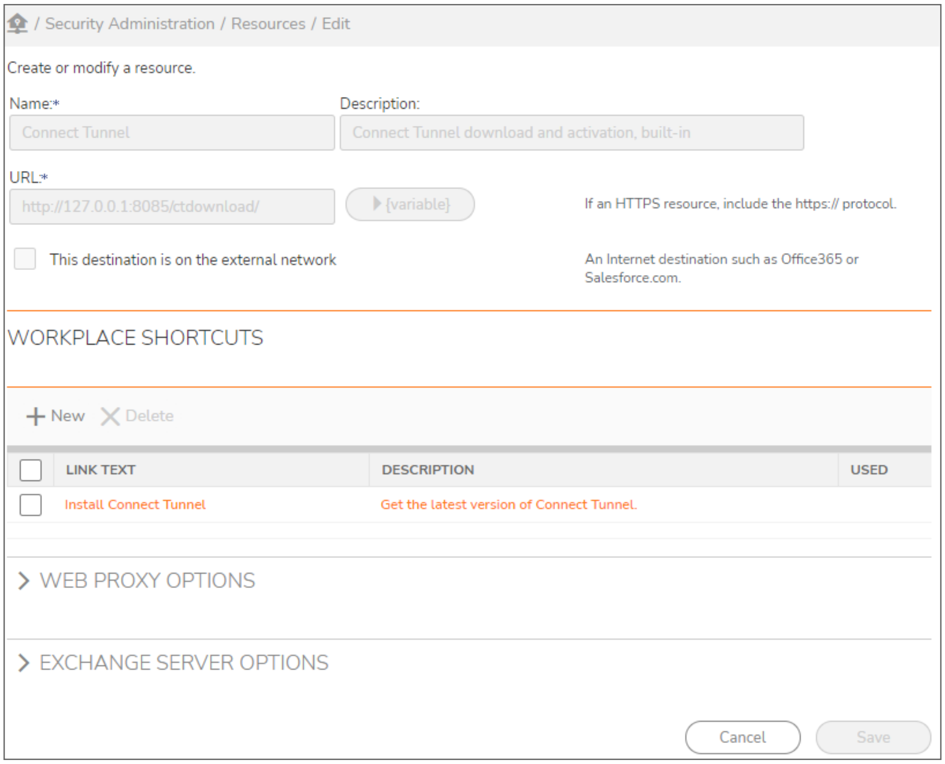
4. For an overview of a particular resource, click the right arrow (▶) next to it. This shows the resource type, its value, and whether it is used by a WorkPlace shortcut or access rule.



□ ▶	TYPE	NAME	DESCRIPTION ↓	USED
▶		WorkPlace	WorkPlace, built-in	✓
▶		Network Explorer	Network Explorer, built-in	✓
▼		Connect Tunnel	Connect Tunnel download and activation, built-in	✓
		Type: URL Value: http://127.0.0.1:8085/ctdownload/	Used by: WorkPlace shortcut: Install Connect Tunnel	
□ ▶		Reference Library		

ⓘ **NOTE:** By default, there are some read-only resource definitions included with the appliance, for example, Secure Mobile Access WorkPlace and Connect Tunnel Download. These definitions are required by the appliance services and cannot be deleted (a read-only resource has no check box next to it).

5. To edit a resource, click its link in the resource list.



/ Security Administration / Resources / Edit

Create or modify a resource.

Name:* Connect Tunnel

Description: Connect Tunnel download and activation, built-in

URL:* http://127.0.0.1:8085/ctdownload/ ▶ {variable}

If an HTTPS resource, include the https:// protocol.

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUTS

+ New ✕ Delete

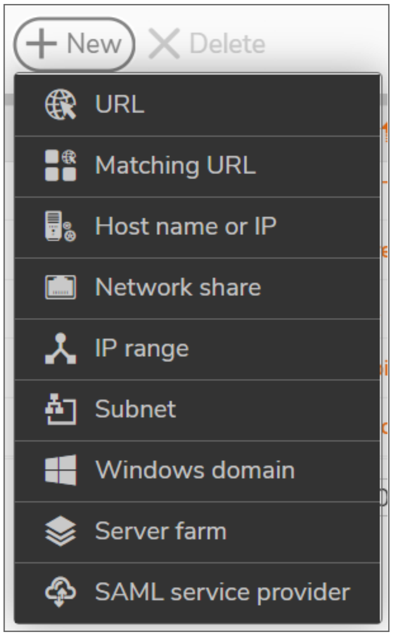
□	LINK TEXT	DESCRIPTION	USED
□	Install Connect Tunnel	Get the latest version of Connect Tunnel.	

Adding Resources

Creating application resources—Web, client/server, and file share resources—is the first step in forming access policies for your users.

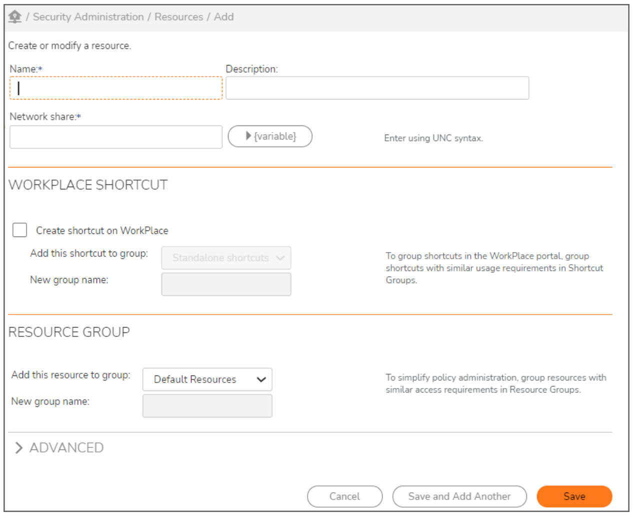
To add a resource:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon and then choose a resource type from the drop-down menu:



3. The **Add Resource** page is displayed.

   The options you see on the **Add Resource** page depend on the resource type you selected.



/ Security Administration / Resources / Add

Create or modify a resource.

Name:*

Description:

Network share:* {variable} Enter using UNC syntax.

WORKPLACE SHORTCUT

□ Create shortcut on WorkPlace

Add this shortcut to group: Standalone shortcuts

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

RESOURCE GROUP

Add this resource to group: Default Resources

New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

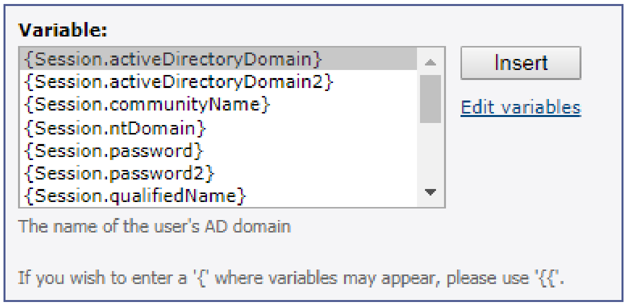
ADVANCED

The options shown in the below table are shared across the specified resource types:

Shared Options

Option	Description	Resource type

Name	Resource name	All
Description	Resource description	All
This destination is on the external network.	Select this option if this resource is on an external network.	

Variable	Select a variable from the menu to define dynamic resources; see Using Variables in Resource and WorkPlace Shortcut Definitions.
	
	Variable:
	{Session.activeDirectoryDomain}
	{Session.activeDirectoryDomain2}
	{Session.communityName}
	{Session.ntDomain}
	{Session.password}
	{Session.password2}
	{Session.qualifiedName}
	Insert
	Edit variables
	The name of the user's AD domain
	If you wish to enter a '{' where variables may appear, please use '{{'.
		- Citrix server farm
		- Domain
		- Host name or IP
		- Matching URL
		- Network share
		- URL

Create shortcut in WorkPlace	Add a shortcut to a Web resource in WorkPlace. The name you assign to the resource will appear in the list of **Shortcuts** on the **Secure Mobile Access WorkPlace** page. You can add the shortcut to a new or existing shortcut group in order to keep shortcuts with similar usage requirements together on the WorkPlace portal page.	- Domain - Network share - URL
Web application profile (Web proxy options or Advanced area)	This list contains preconfigured Web profiles that are recommended for several popular Web applications, custom Web profiles, and a default Web profile. If you are unsure about which profile to select, choose *Default*. To see a profile, click **View selected profile**. Also see Adding Web Application Profiles.	- Domain - Host name or IP - IP range - Matching URL - Subnet - URL

The options shown in the below table are unique to the URL resource type:

URL Resource Type Unique Options

Option	Description

URL	If you do not enter a protocol identifier, AMC automatically inserts `http://before` the URL. If this is a URL for a secure site, you must include the `https://protocol` identifier. For example, type `https://example.domain.com`.
Alias name (Web proxy)	Specify a public alias to represent a private URL. The alias name is visible to users— make it short and descriptive so that it is easy to remember. You should specify an **Alias name** if: • You want to obscure the internal host name for this resource. • The URL resource is not contained within a search domain configured for **Name resolution** on the **Network Settings** page. • You normally redirect traffic through a network agent, but in this case you want to force the resource to be proxied using translated Web access. See Adding Web Shortcuts for more information. ⓘ | **NOTE:** • The private URL that you are representing with the alias must point to a directory on the back-end server, not a particular file. • Use ASCII characters when specifying an alias. Users who connect to WorkPlace using translated Web access will see an error message if non-ASCII characters are used. • Creating an alias works only for URLs (addresses with an `http` or `https` prefix); you cannot specify an alias for a UNC path or FTP resource (`ftp://`), for example. Also see Example: Specifying a URL Alias for a detailed description of how an alias is used.
Port (Web proxy)	The **Port** option is available when you select **Access this resource on a custom port** under **Custom access**. Enter the custom port number. The resource becomes available at that port on each WorkPlace site. The port must be open on any firewalls and must not be already in use on the external side of the appliance. Actual delivery of Web content depends on policy checks in accordance with normal appliance operation.

Custom FQDN (Web proxy)	The **Custom FQDN** option is available when you select **Access this resource using a custom FQDN** under **Custom access**. Type the **Custom FQDN name** (such as `custom.mydomain.com`) to be hosted by an externally accessible Web server on the appliance. By default, AMC listens on all interfaces for all services and connects the request to the correct service based on the FQDN being requested. The host name cannot be relative to any WorkPlace site. A maximum of 32 IPv4 or IPv6 addresses for externally defined host names are allowed between independently hosted Web application names and WorkPlace sites, supporting up to 64 total host names. Custom FQDN mapped Web access provides Single Sign-on support. If the host name or IP address on the certificate does not match the Custom FQDN or IP address that you specified for this site, a security warning is displayed when users access the site. Custom FQDNs are handled similar to configuring a WorkPlace site, as explained in Adding WorkPlace Sites.
Synonyms (Web proxy)	Define alternative names for the URL resource name. This is convenient for users if they access the server using a different name (perhaps an unqualified or condensed name), or if a Web page contains links pointing to a DNS alias and the name is not properly translated by the Web proxy service. Separate multiple synonyms with semicolons. The appliance automatically defines a shortened name for the resource as a synonym. For example, if the URL is `http://mail.example.com`, the appliance adds the synonym mail. This synonym does not, however, appear in the **Synonyms** field. When **Translate this resource** is selected and you specify **Synonyms**, there must be something in the **Alias name** field. For the other Custom access options, the **Synonyms**field is independent of other fields.

Provide Exchange ActiveSync and Outlook Anywhere access to this resource (Exchange Server)	Select this check box to allow Exchange ActiveSync and Outlook Anywhere access to this resource. For more information, see Exchange ActiveSync access. For an example use case, see Example: Supporting Exchange on iPhones. For Outlook Anywhere, see Configuring SMA Support for Microsoft Outlook Anywhere.
Exchange server FQDN (Exchange Server)	Type the **Exchange server FQDN** (IPv4 or IPv6) name (such as `custom.mydomain.com`) to be hosted by an externally accessible Web server on the appliance.
Realm (Exchange Server)	Select the realm from the drop-down list. ActiveSync access requires the use of a realm that uses a single Active Directory authentication server. The realm must be already configured.
Fallback Exchange server URL (Exchange Server)	Enter the URL for the Exchange Server you want to use as the fallback server.

The options shown in the below table are unique to the **Matching URL** resource type.

Matching URL Resource Type Unique Options

Option	Description

URL	If you do not enter a protocol identifier, AMC automatically inserts `http://before` the URL. If this is a URL for a secure site, you must include the `https://`protocol identifier. For example, type `https://example.domain.com`. The wildcard characters “*” and “?” can be used within address segments (between periods) of a **Matching URL** resource. Do not use the “?” character after the domain name—it indicates a URL query string. Use wildcard characters in the following situations: • Type `www.yourcompany*.com` to reference several domains that begin with `yourcompany` and end with `.com`, or type `www.yourcompany.*` to reference both `http://www.yourcompany.com` and `http://www.yourcompany.de`. • Create an entry, such as `mail*.yourcompany.com`, that gives the user access to anything in the `yourcompany` domain that begins with `mail`. This example provides access to `mail.yourcompany.com` and `mail2.yourcompany.com`, but not to `mail3.wemmet.yourcompany.com`. The URL is not case-sensitive. ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.
Path and query string matching	These options allow you to block email attachments, or prevent a Web-based application from displaying restricted data by matching a path element or query string value to a particular URL. SeeExample: Blocking Email Attachments and Example: Restricting Access to Sensitive Data for more information. The **Query string** value is case-sensitive, while the **Path element** is not.

The options shown in the below table are unique to the **Host name or IP** resource type:

Host Name Or IP Resource Type Unique Options

Option	Description

Host name or IP	A host can include any computer on your network; for example, bart.private.example.com or 192.0.34.72. When you specify a host name, the wildcard characters “*” and “?” can be used within an address segment (between periods). For example, the entry mail*.yourcompany.com gives the user access to anything in the yourcompany domain that begins with mail (for example, (mail.yourcompany.com and mail2.yourcompany.com), but not to mail3.wemmet.yourcompany.com. The host name is not case-sensitive. ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

The option shown in the below table is unique to the **Network share** resource type:

Network Share Resource Type Unique Options

Option	Description
Network share	Type a UNC path. This can be an entire server (for example, \\ginkgo), a shared folder (\\john\public), or a network folder (\\ginkgo\news).

The option shown in the below table is unique to the **IP range** resource type:

IP Range Resource Type Unique Options

Option	Description
IP range	An IP range typically identifies a partial range of computers within a subnet; for example, 192.0.34.72-192.0.34.74.

The options shown in the below table is unique to the **Subnet** resource type:

Subnet Resource Type Unique Options

Option	Description
Subnet IP	A subnet is a portion of a network that shares a common address component. For example, 192.26.34.0.
Subnet mask	For example, 255.255.255.0.

The options shown in the below table are unique to the **Domain** resource type:

Domain Resource Type Unique Options

Option	Description

Domain	A domain encompasses one or more hosts. If the **Windows domain** check box is cleared, the domain name must be in DNS syntax. For example, `sampledomain.com`.
Windows domain	To define an entire Windows domain, select the **Windows domain** check box, and then type the name of the **Domain** in either NetBIOS or DNS syntax (such as `example` or `example.com`). Defining a domain gives authorized users access to all the network file resources within the domain.

The option shown in the below table is unique to the **Server farm** resource type:

Server Farm Resource Type Unique Option

Option	**Description**
Server farm list	Specify the **Host name or IP address** and service **Port** of up to six Citrix servers running the XML service or VMware servers running the XML service or VMware servers running the broker service. For more information, see Adding Citrix Server Farm Resources or Adding VMware View Resources.

4. After you've finished defining a resource, click **Save**.

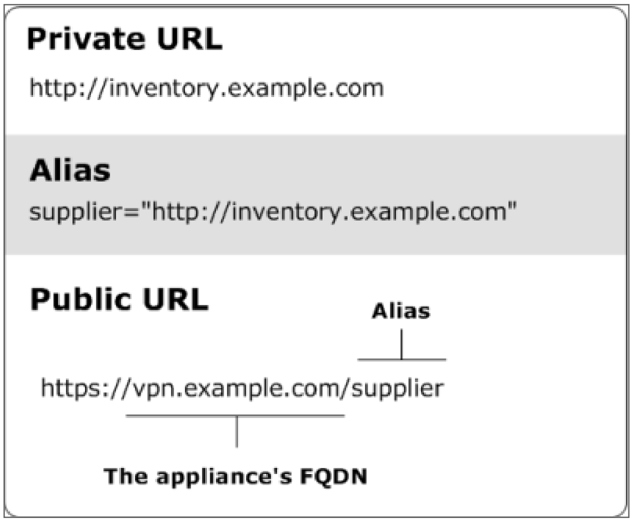
Example: Specifying a URL Alias

Any Web resource—such as a Web application, a Web portal, or a Web server—can be defined as a URL resource. Defining a Web resource as a URL provides several advantages:

- You can create a Web shortcut for WorkPlace to give users quick access to a URL resource.
- You can define very specific access rules to control which users can access the URL.
- You have the option of obscuring (or "aliasing") the internal host name so it is not publicly exposed. When a user accesses an alias, the request is proxied to the downstream Web resource and its private URL is translated using the alias you specify. The user sees only the public (or aliased) URL.

The below image illustrates how the private address for an inventory application might be translated into a public URL.

Private Address Translated To A Public URL


Private URL
http://inventory.example.com
Alias
supplier="http://inventory.example.com"
Public URL
Alias
https://vpn.example.com/supplier
The appliance's FQDN

The private URL for this resource is http://inventory.example.com, and the administrator has created an alias for it named supplier.

Instead of using the private URL (which would publicly expose a sensitive host name), suppliers access a public URL: https://vpn.example.com/supplier.

A public URL consists of the following:

- An https:// prefix rather than http://: this is because all traffic to and from the SMA appliance is secured using SSL
- The appliance’s fully qualified domain name (in this example, vpn.example.com)
- The resource’s alias name (in this example supplier)

ⓘ | **NOTE:**

- Some Web-based applications use JavaScript or other browser extensions that submit traffic using protocols other than HTTP. Examples of such applications include Citrix XenApp and certain versions of SAP. Although accessed using a Web browser, these applications may need to be defined as a client/server resource and proxied through OnDemand using the client/server access service.
- The private URL for which you create an alias must be a directory on the back-end server; it cannot be a file, and it must begin with either http:// or https://.
- Use ASCII characters when specifying an alias. Users who connect to WorkPlace using translated Web access will see an error message if non-ASCII characters are used.
- For information on defining URL resources, see Adding Resources.

Example: Blocking Email Attachments

Your organization may need to restrict access to sensitive data for users working from an unmanaged or untrusted public system. For example, you may want to allow users to view email messages, but prevent them from downloading email attachments that could be left behind on the computer and accessible to unauthorized users.

The following example demonstrates how to use an access control rule, together with a **Matching URL** resource and End Point Control zone, to block attachments from being downloaded to untrusted devices. For an overview of access control, see Access Control Rules.

The example assumes that you have an EPC zone configured (named *Untrusted* in this example) into which devices that are not IT-managed are classified; see Managing EPC with Zones and Device Profiles for information about configuring and using zones.

To block email attachments using a Matching URL resource:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon.

   The **Add Access Rule** page displays.
3. In the **Position** field, type a number to specify the rule's position in the access rule list.
4. Use the **Action** buttons to specify **Deny**.

   This will deny users access to any resource that matches the pattern you specify in the next step.
5. Complete the information under **Basic settings**:
   a. Leave **User** selected (so that the rule users trying to access a resource).
   b. The **From** field specifies the users to whom the rule applies. For this example, leave the value as **Any user**.
   c. In the **To** field, click **Edit** to specify the target resource for this rule.

      A Resources window appears.
   d. Click **New**, and then select **Matching URL**.

      The **Add Resource** - **Matching URL** page displays.
   e. Type a name for the resource. For example, `Block email attachments`.
   f. In the **URL** box, type the URL address of your mail server.
   g. In the **Path and query string matching** area, select **Exchange/OWA attachments** from the **Type of match** list.
   h. Click **Save**.
6. In the **End Point Control zones** area, click **Edit** to select the zone from which you will deny access to the resource (*Untrusted*).
7. When you create a rule that specifies a Matching URL resource type, the user must be allowed to use a browser as an access method. On the **Advanced** tab, in the **Access method restrictions** area, make sure that the **Client software agents** are either set to **Any**, or that **Web browser** is among the selected agents.
8. Click **Finish**.

   ⓘ | **NOTE:**

- Some Web-based applications automatically redirect users to other Web pages. Be certain to use the target URL address (the Web page to which users are redirected) when configuring the appliance to block email attachments. See Example: Working with a URL Redirect for more information.
- You cannot configure a Matching URL resource to block attachments for users who connect to the appliance using OnDemand Tunnel or Connect Tunnel.

Example: Supporting Exchange on iPhones

Exchange ActiveSync Email and related functions are supported on Android, Apple iPad, and Apple iPhone.

The following example describes configuring a URL resource to support iPhone users who wish to access Microsoft Exchange.

ⓘ | **NOTE:** This example assumes you have a realm which uses single Active Directory authentication.

Allow iPhone users to access corporate Exchange server:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon.
3. Select **URL** from the drop-down list.

   The **Add Resource - URL** page displays.
4. Enter the name, description, and externally-facing URL. Enter only the server name without a starting or index page. In this example, we will use `internalexchangeserver.SMA.com`.
5. Choose a group to add this resource to. In this example, we have left this in the default group.
6. Click **Exchange Server options**.

   The **Exchange Server options** section appears.
7. Select the **Enable Exchange ActiveSync and Outlook Anywhere access to this resource** check box.
8. In the **Host and domain name** field, type the external host name and domain that will be accessed by iPhone users.
9. Select the realm from the **Realm** drop-down menu.

   Only realms that use Active Directory for authentication are available as choices.
10. Click **Save**.
11. To configure an ActiveSync device profile for iPhones, click **End Point Control in** the main navigation menu in AMC.
12. On the **Device Profiles** tab, click **New** and select **Exchange Activesync**.
13. Enter a name and description for the device profile in the **Name** and **Description** fields.
14. In the **Add attribute(s)** section, select **Equipment ID** for the **Type**.
15. In the **Device identifier** field, enter the user attribute variable that contains the device identifier. For iPhone, the identifier is the serial number of the device. For details, see the **Equipment ID table** under Device Profile Attributes.

16. Click **Save**.
17. Notify your iPhone users of the externally-facing URL and instruct them to log in using their Active Directory credentials. Users must configure ActiveSync for Exchange on the device:
    a. On the iPhone, navigate to **Settings > Mail > Contacts and Calendars > Add Account > User's account info**.
    b. Set the server name to the URL (external host name and domain) provided by the administrator.

ⓘ **NOTE:** To ensure that your Exchange server is correctly configured to work with iPhones, it is recommended that you test iPhone access with the Exchange server directly. After confirming iPhone access to email, then add the SMA appliance between the iPhone and the Exchange server. If your Exchange server is not accessible from the Internet, you can set up a WiFi access point to test iPhone access to it.

Example: Restricting Access to Sensitive Data

The following example demonstrates how to use an access control rule, together with a Matching URL resource and End Point Control zone, to prevent a Web-based application from displaying restricted data to untrusted devices.

- For an overview of access control, see Access Control Rules.
- The example assumes that you have an EPC zone configured (named *Untrusted* in this example) into which devices that are not IT-managed are classified; see Managing EPC with Zones and Device Profiles for information about configuring and using zones.

Prevent a Web-based application from retrieving data using a Matching URL resource:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon.
   The **Add Access Rule** page displays.
3. In the **Position** field, type a number to specify the rule's position in the access rule list.
4. Use the **Action** buttons to specify **Deny**.
   This will deny users access to any resource that matches the pattern you specify in the next step.
5. Complete the information under **Basic settings**:
   a. Leave **User** selected (so that the rule applies to users trying to access a resource).
   b. The **From** field specifies the users to whom the rule applies. For this example, leave the value as *Any user*.
   c. In the **To** field, click **Edit** to specify the target resource for this rule.
   A **Resources** page displays.
   d. Click the **+** (New) icon.
   e. Select **Matching URL**. The **Add Resource - Matching URL** page displays.
   f. Type a name for the resource. For example, `Patient Records`.

g. In the **URL** field, type the URL address of your Web-based application. For example, `www.patient-records.com`.

h. In the **Path and query string matching** area, select *Custom* from the **Type of match** list.

i. Click the **+** (New) icon.

j. Select **Path element**. Type `reports.aspx`. (The path is not case-sensitive.)

k. Click **OK**.

l. Click the **+** (New) icon.

m. Select **Query string**. Type `last_name=`. (The query string is case-sensitive.)

n. Click **OK**

o. Click **Save**.
   The **Add Resource - Matching URL** closes.

6. In the **End Point Control zones** section, click **Edit** to select the zone from which you will deny access to the resource (**Untrusted**).
7. When you create a rule that specifies a Matching URL resource type, the user must be allowed to use a browser as an access method. On the **Advanced** tab, in the **Access method restrictions** area, make sure that the **Client software agents** are either set to **Any**, or that **Web browser** is among the selected agents.
8. Click **Finish**.

After you save and apply your changes, users who attempt to open the Patient Records resource (using a URL that matches `http://www.patient-records.com/reports.aspx?last_name=`) and who are classified into the **Untrusted** zone will be denied access.

ⓘ | **NOTE:**

- Some Web-based applications automatically redirect users to other Web pages. Be certain to use the target URL address (the Web page to which users are redirected) when configuring the appliance to block email attachments. See Example: Working with a URL Redirect for more information.
- You cannot configure a Matching URL resource to restrict access to sensitive data for users who connect to the appliance using OnDemand Tunnel or Connect Tunnel.

Editing Resources

Before modifying a resource, carefully examine any **Access Control** rules associated with it to understand how your changes will affect your security policy.

To edit a resource:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the name of the resource that you want to edit.
3. On the **Edit Resource** page, make your edits as needed.
4. Click **Save**.

NOTE: You cannot change an existing client/server resource’s definition setting (for example, change a host name to an IP range); instead, you must create a new resource and apply the appropriate definition setting.

Deleting Resources

You cannot delete a resource that is referenced in an access control rule, resource group, or WorkPlace shortcut. Before deleting a resource, you must first remove it from any rules in which it is referenced. See Deleting Referenced Objects for more details.

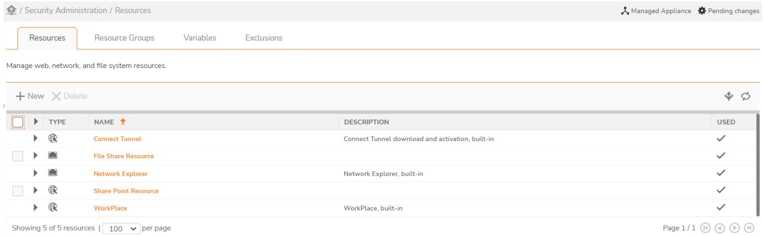
To delete a resource:

1. In the AMC, navigate to **Security Administration > Resources**.
2. On the **Resources** page, select the check box to the left of any resources that you want to delete.
3. Click the **Delete** button.

Configuring a Resource as a SharePoint Web Service

To configure a resource as a SharePoint Web Service:

1. In the AMC, navigate to **Security Administration > Resources**.



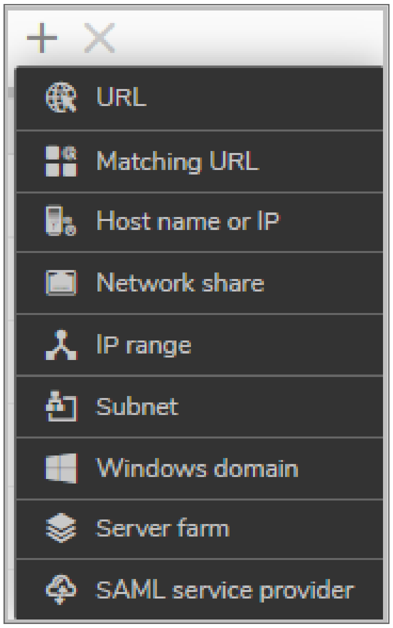
Manage web, network, and file system resources.

TYPE	NAME	DESCRIPTION	USED
	Connect Tunnel	Connect Tunnel download and activation, built-in	✓
	File Share Resource		✓
	Network Explorer	Network Explorer, built-in	✓
	Share Point Resource		✓
	WorkPlace	WorkPlace, built-in	✓

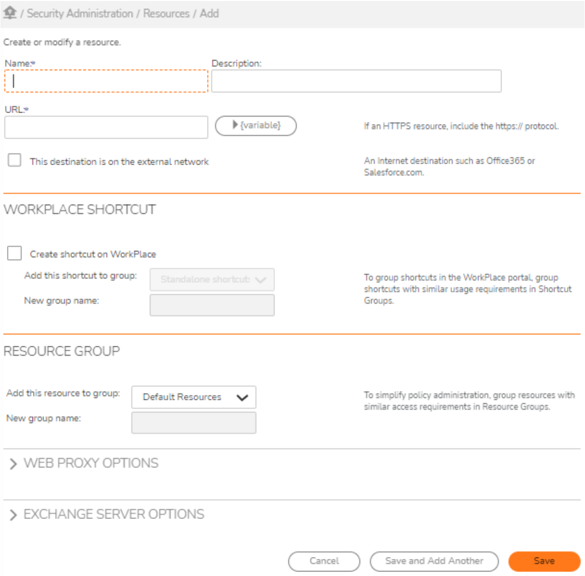
Showing 5 of 5 resources | 100 per page

Page 1 / 1

2. Click click the **+** (New) icon.
3. Select **URL** from the drop-down list.



The **Add Resource - URL** page displays.


/ Security Administration / Resources / Add

Create or modify a resource.

Name*

Description:

URL*

If an HTTPS resource, include the https:// protocol.

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUT

□ Create shortcut on WorkPlace

Add this shortcut to group: Standalone shortcut

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

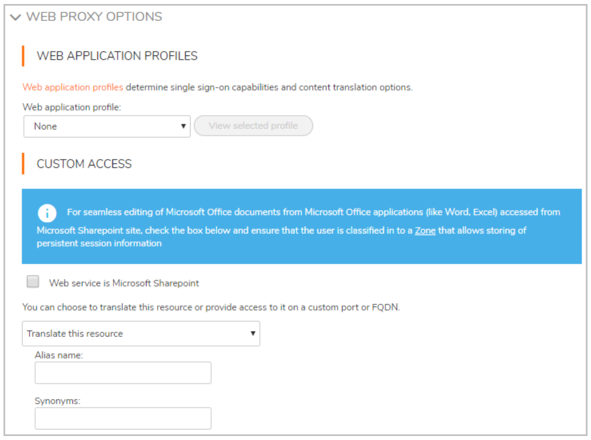
RESOURCE GROUP

Add this resource to group: Default Resources

New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

4. Enter the **Name** and the **URL** for this resource.
5. If this resource is on the external network, select the checkbox for **This destination is on the external network**.
6. Scroll down to the **Web Proxy Options** section and expand it.



WEB PROXY OPTIONS

WEB APPLICATION PROFILES

Web application profiles determine single sign-on capabilities and content translation options.

Web application profile: None

CUSTOM ACCESS

For seamless editing of Microsoft Office documents from Microsoft Office applications (like Word, Excel) accessed from Microsoft Sharepoint site, check the box below and ensure that the user is classified in to a Zone that allows storing of persistent session information

□ Web service is Microsoft Sharepoint

You can choose to translate this resource or provide access to it on a custom port or FQDN.

Translate this resource

Alias name:

Synonyms:

7. From the **Web application profile** drop-down menu, select **SharePoint**.
8. Select the **Web service is Microsoft Sharepoint** checkbox.
9. Select **Access this from resource using a custom FQDN**.
10. In the **Custom FQDN** field, enter the FQDN.

Exclusions

Resource Exclusion List feature is enhanced and renamed as **Exclusions** from 12.4.1 version onwards. Exclusion excludes host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance.

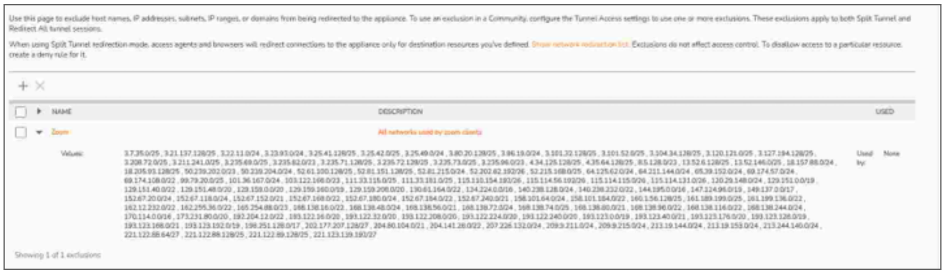
An Exclusion is a named list of:

- Addresses
- Address ranges
- Networks (supports slash format)
- Domain names (wildcards supported)

An Exclusion does not have any effect unless used by a community. It can be public or private names/addresses or names resolved by an appliance.

To use an exclusion in a Community, configure the **Tunnel Access** settings to use one or more exclusions. These exclusions apply to both Split Tunnel and Redirect All Tunnel sessions.

When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources which you have defined.



Use this page to exclude host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance. To use an exclusion in a Community, configure the Tunnel Access settings to use one or more exclusions. These exclusions apply to both Split Tunnel and Redirect All tunnel sessions.

When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources you've defined. Show network redirection list. Exclusions do not affect access control. To disallow access to a particular resource, create a deny rule for it.

□	NAME	DESCRIPTION	USED
□	Zoom	All networks used by zoom clients	

Values: 3.7.35.0/25 , 3.21.137.128/25 , 3.22.11.0/24 , 3.23.93.0/24 , 3.25.41.128/25 , 3.25.42.0/25 , 3.25.49.0/24 , 3.80.20.128/25 , 3.96.19.0/24 , 3.101.32.128/25 , 3.101.52.0/25 , 3.104.34.128/25 , 3.120.121.0/25 , 3.127.194.128/25 , 3.208.72.0/25 , 3.211.241.0/25 , 3.235.69.0/25 , 3.235.82.0/23 , 3.235.71.128/25 , 3.235.72.128/25 , 3.235.73.0/25 , 3.235.96.0/23 , 4.34.125.128/25 , 4.35.64.128/25 , 8.5.128.0/23 , 13.52.6.128/25 , 13.52.146.0/25 , 18.157.88.0/24 , 18.205.93.128/25 , 50.239.202.0/23 , 50.239.204.0/24 , 52.61.100.128/25 , 52.81.151.128/25 , 52.81.215.0/24 , 52.202.62.192/26 , 52.215.168.0/25 , 64.125.62.0/24 , 64.211.144.0/24 , 65.39.152.0/24 , 69.174.57.0/24 , 69.174.108.0/22 , 99.79.20.0/25 , 101.36.167.0/24 , 103.122.166.0/23 , 111.33.115.0/25 , 111.33.181.0/25 , 115.110.154.192/26 , 115.114.56.192/26 , 115.114.115.0/26 , 115.114.131.0/26 , 120.29.148.0/24 , 129.151.0.0/19 , 129.151.40.0/22 , 129.151.48.0/20 , 129.159.0.0/20 , 129.159.160.0/19 , 129.159.208.0/20 , 130.61.164.0/22 , 134.224.0.0/16 , 140.238.128.0/24 , 140.238.232.0/22 , 144.195.0.0/16 , 147.124.96.0/19 , 149.137.0.0/17 , 152.67.20.0/24 , 152.67.118.0/24 , 152.67.152.0/21 , 152.67.168.0/22 , 152.67.180.0/24 , 152.67.184.0/22 , 152.67.240.0/21 , 158.101.64.0/24 , 158.101.184.0/22 , 160.1.56.128/25 , 161.189.199.0/25 , 161.199.136.0/22 , 162.12.232.0/22 , 162.255.36.0/22 , 165.254.88.0/23 , 168.138.16.0/22 , 168.138.48.0/24 , 168.138.56.0/21 , 168.138.72.0/24 , 168.138.74.0/25 , 168.138.80.0/21 , 168.138.96.0/22 , 168.138.116.0/22 , 168.138.244.0/24 , 170.114.0.0/16 , 173.231.80.0/20 , 192.204.12.0/22 , 193.122.16.0/20 , 193.122.32.0/20 , 193.122.208.0/20 , 193.122.224.0/20 , 193.122.240.0/20 , 193.123.0.0/19 , 193.123.40.0/21 , 193.123.176.0/20 , 193.123.128.0/19 , 193.123.168.0/21 , 193.123.192.0/19 , 198.251.128.0/17 , 202.177.207.128/27 , 204.80.104.0/21 , 204.141.28.0/22 , 207.226.132.0/24 , 209.9.211.0/24 , 209.9.215.0/24 , 213.19.144.0/24 , 213.19.153.0/24 , 213.244.140.0/24 , 221.122.88.64/27 , 221.122.88.128/25 , 221.122.89.128/25 , 221.123.139.192/27

Used by: None

Showing 1 of 1 exclusions

For more information on how to configure Exclusions, see Using the Exclusions.

Using the Exclusions

By default, access agents and Web browsers redirect connections through the appliance for destination resources that you've defined in AMC. This redirection is a little different, depending on the user's means of access:

- The tunnel access agent redirects connections through the appliance for any destination resource that the user is permitted to access.
- A Web browser redirects to the appliance all destination resources that have been defined in AMC; if the user does not have access, a "permission denied" Web page is displayed.

Use the Exclusions page to configure exclusions to prevent host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance. To use an exclusion in a Community, configure the Tunnel Access settings to use one or more exclusions. Exclusions configured for a community apply to both tunnel sessions as well as browser sessions.

When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources you've defined. Exclusions do not affect access control or security. To disallow access to a particular resource, create a deny rule for it.

There may, however, be resources that you don't want redirected through the appliance. The most common examples are Office365 and Zoom not being redirected through the appliance.

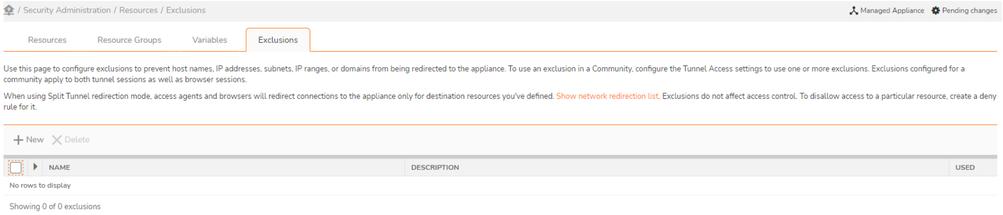
For example, a user starts Outlook Web Access through the appliance and reads an email message with a link to a public site that is within a domain resource configured on the appliance. The traffic generated by following that link would be sent through the appliance. You can prevent this by specifying the public resource in the exclusion list.

Use the exclusions to specify any resources (including host names, IP addresses, or domains) from being redirected through the appliance. When specifying a domain, you can also use the wildcard characters asterisk (`*`) and question mark (`?`). This list is global and all access services.

ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

ⓘ **NOTE:** You should define the corresponding IP/Range/Subnet in Wildcard exclusion.

To see which resources are configured to be redirected through the appliance, click the **Show network redirection list** link. This displays the **Redirection List** page.



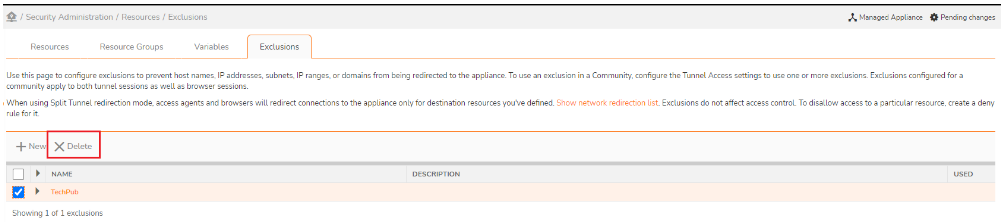
Use this page to configure exclusions to prevent host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance. To use an exclusion in a Community, configure the Tunnel Access settings to use one or more exclusions. Exclusions configured for a community apply to both tunnel sessions as well as browser sessions.

When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources you've defined. Show network redirection list. Exclusions do not affect access control. To disallow access to a particular resource, create a deny rule for it.

□	NAME	DESCRIPTION	USED
No rows to display			

Showing 0 of 0 exclusions

To delete a resource from the exclusions, select its checkbox and then click **Delete** icon.



Use this page to configure exclusions to prevent host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance. To use an exclusion in a Community, configure the Tunnel Access settings to use one or more exclusions. Exclusions configured for a community apply to both tunnel sessions as well as browser sessions.

When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources you've defined. Show network redirection list. Exclusions do not affect access control. To disallow access to a particular resource, create a deny rule for it.

□	NAME	DESCRIPTION	USED
☑	TechPub		

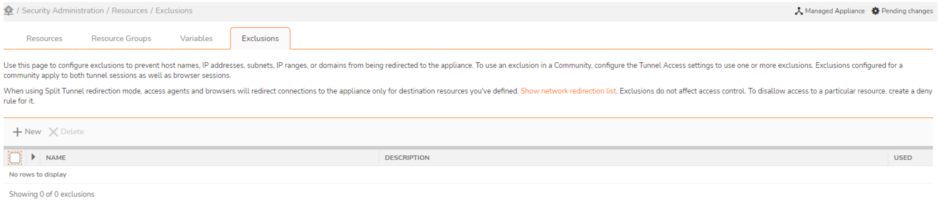
Showing 1 of 1 exclusions

If you exclude a resource by specifying its fully qualified domain name (FQDN), users who connect to WorkPlace from a realm that provides access using translated Web mode can still access the resource if they type its unqualified domain name in the WorkPlace **Intranet Address** field.

To add a resource to the exclusions:

△ **CAUTION: If you create a Domain resource in AMC (for example, win.yourcompany.com) and you exclude a resource from that domain using its IP address (10.20.30.40), the resource can still be accessed using its FQDN (server.win.yourcompany.com). This note of caution applies only to agents that use the Web proxy service, not the tunnel clients.**

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **Exclusions** tab.



Use this page to configure exclusions to prevent host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance. To use an exclusion in a Community, configure the Tunnel Access settings to use one or more exclusions. Exclusions configured for a community apply to both tunnel sessions as well as browser sessions.

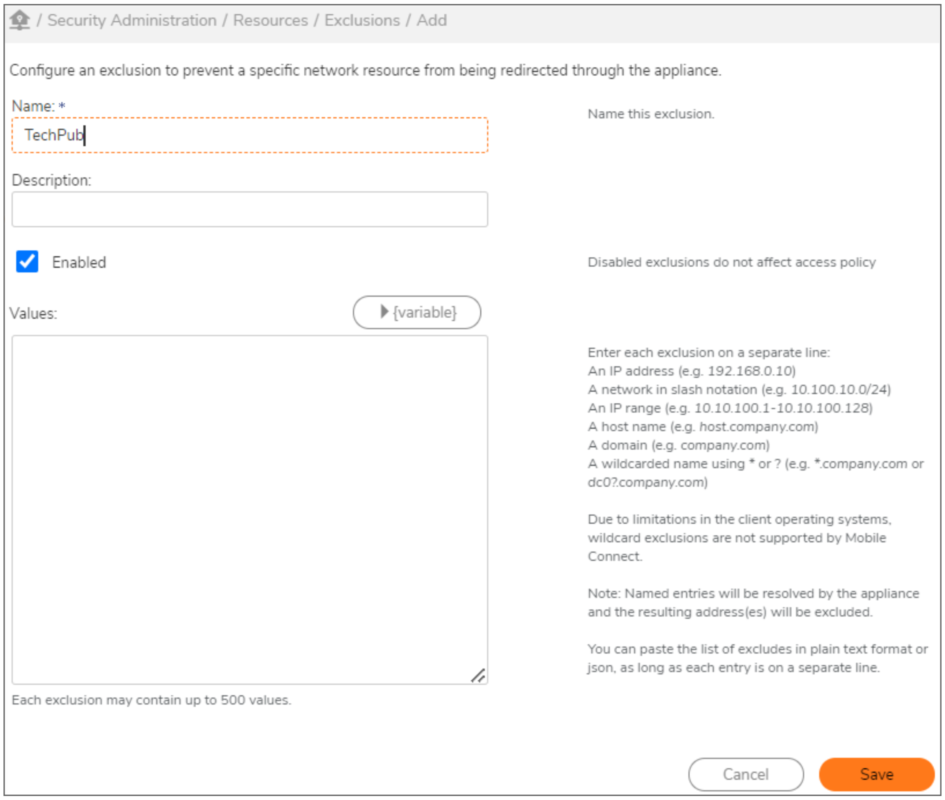
When using Split Tunnel redirection mode, access agents and browsers will redirect connections to the appliance only for destination resources you've defined. Show network redirection list. Exclusions do not affect access control. To disallow access to a particular resource, create a deny rule for it.

□	NAME	DESCRIPTION	USED
No rows to display			

Showing 0 of 0 exclusions

3. Click + (new) icon.

   The **Add Exclusion** page displays.



/ Security Administration / Resources / Exclusions / Add

Configure an exclusion to prevent a specific network resource from being redirected through the appliance.

Name: * TechPub — Name this exclusion.

Description:

☑ Enabled — Disabled exclusions do not affect access policy

Values:

Enter each exclusion on a separate line:
An IP address (e.g. 192.168.0.10)
A network in slash notation (e.g. 10.100.10.0/24)
An IP range (e.g. 10.10.100.1-10.10.100.128)
A host name (e.g. host.company.com)
A domain (e.g. company.com)
A wildcarded name using * or ? (e.g. *.company.com or dc0?.company.com)

Due to limitations in the client operating systems, wildcard exclusions are not supported by Mobile Connect.

Note: Named entries will be resolved by the appliance and the resulting address(es) will be excluded.

You can paste the list of excludes in plain text format or json, as long as each entry is on a separate line.

Each exclusion may contain up to 500 values.

4. (Optional). Enter the description for the Exclusion.
5. Select the **Enabled** check box to allow the access to those created exclusions.

   ⓘ | **NOTE:** Disabled exclusions do not exclude anything.

6. In the **Values** field, enter the host names, IP addresses, subnets, IP ranges, or domains that you want to exclude from being redirected through the appliance.

   ⓘ | **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

   For example, if you have three public web servers (www.YourCompany.com, www2.YourCompany.com, and www3.YourCompany.com), you can allow the network traffic associated with them to avoid the appliance, which will improve performance. Add all three public sites to the Exclusions by using a wildcard character: www?.YourCompany.com. Resources in this list can also contain variables; see Using Variables in Resource and WorkPlace Shortcut Definitions for more information.

   ⓘ | **NOTE:** Migration of prior versions of SMA that contains Resource Exclusion List to 12.4.1:

   - All entries in Resource Exclusion List migrate to a single exclusion named Split Tunnel
   - All Split tunnel communities use this exclusion named Split Tunnel
   - For Redirect All communities, exclusions will not be migrated, which may affect browser-only sessions

7. Click **Save**.

Using Variables in Resource and WorkPlace Shortcut Definitions

Using variables, you can define a single resource or WorkPlace shortcut that derives its value from a property that is unique for each user. Variables can be defined by a property associated with the session a user has started (the user name, for example, or the name of the zone to which he or she has been assigned), or by querying an external LDAP store for a specific set of attributes, such as a group or computer name.

Variables can be used for all resource types except **IP range** and **Subnet**. If a variable resolves to nothing, any configuration item using it will be undefined. For example, you might query an LDAP store for a user's IMEI number (the built-in ID number on a mobile device). In the case of a user who does not have an IMEI number, the variable would not resolve to anything during that user session. A WorkPlace shortcut that uses the variable would not be displayed, for example, and a policy rule that uses it will also fail.

Topics:

Using Session Property Variables

After a user has started a WorkPlace session by logging in, there are several session properties that are known, such as the name of the community to which the user has been assigned. You can use these properties to create dynamic resources.

For example, you might want mobile users to have access to a different network share than users with desktop computers. The way you would do this is as roughly as follows:

- Define two communities (*Mobile* and *Desktop*).
- Set up two file shares on your network. For example, \\*company**Mobile* and \\*company**Desktop*.
- Define a resource for WorkPlace: \\*company**{Session.communityName}*.

A single resource can in this manner present both kinds of users with the link that's appropriate for their devices. Use the variables in the below table.

Built-in Variables

Built-in variables	Description
{Session.activeDirectoryDomain}	The FQDN or IP address of the AD domain to use as a search base.
{Session.activeDirectoryDomain2}	The FQDN or IP address of a second AD domain to use as a search base (if you're using chained authentication).

{Session.communityName}	The name of the community to which the user was assigned when he or she logged in. The community controls which access agents are available and the end point.
{Session.ntDomain}	The login domain. For example, `server3` in this FQDN: `server3.uk.company.com`.
{Session.password}	The password from the first authentication method.
{Session.password2}	The password from the second authentication method, if used.
{Session.qualifiedName}	For your primary (or only) authentication method, this is the fully qualified user name (`username@userdomain.company.com`).
{Session.qualifiedName2}	For your secondary authentication method, this is the fully qualified user name.
{Session.realmName}	The name of the realm the user is logged in to.
{Session.remoteAddress}	The IPv4 or IPv6 address of the user's host as seen by the appliance.
{Session.userName}	The short name for the user from the first authentication method. The short name is usually used for both the user's email address and home folder.
{Session.userName2}	The user's short name from the second authentication method, if used.
{Session.zoneName}	The name of the zone to which the user has been assigned, based on the profile of his or her device.
{Session.ssoUserName}	The user name for single sign-on.
{Session.ssoPassword}	The password for single sign-on.
{URL_REF_VALUE}	The value of the first variable in the URL of a shortcut.

To create a WorkPlace shortcut to a network share based on user name:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon.
3. Select **Network share** from the dropdown list.

4. Give this resource a name (for example, `Personal Folder`), and then type the UNC path for the user folders on your network in the **Network share** field. For example, `\\marine_lab\users\`.
5. Click **{variable}** and select **Session.userName** to add a variable that represents the short login name for the user. When you click **Insert**, the entry for **Network share** looks like this: `\\marine_lab\users\{Session.userName}`
6. Select the **Create shortcut on WorkPlace** check box, and then click **Save**. By default, the resource you created will be displayed as a link in WorkPlace titled **Personal Folder**. If you want to change the link text, go to the **WorkPlace** page in AMC, and then click the link for the new shortcut.

When the user `jdoe` connects to WorkPlace, the variable is automatically replaced with the name entered during login and provides access to a folder named `\\marine_lab\users\jdoe`. When user `rsmith` follows the same link, he has access to the `\\marine_lab\users\rsmith` folder.

ⓘ | **NOTE:**

- For instructions on defining a new variable based on an LDAP query, see Using Query-Based Variables.
- There is an additional built-in variable named `{URL_REF_VALUE}`, which is the value of the first variable in the URL of a shortcut. See Displaying a Series of Shortcuts Using a Single Definition for an example of how to use this.

Using Query-Based Variables

When you configure a realm to use an Active Directory or LDAP authentication server, resources can be defined by querying the external LDAP store for a specific attribute or set of attributes. For example, you can use an LDAP query to create a single resource offering each user a WorkPlace link to his or her personal desktop from home or elsewhere, using the remote desktop protocol (RDP) that is built into Windows.

Topics:

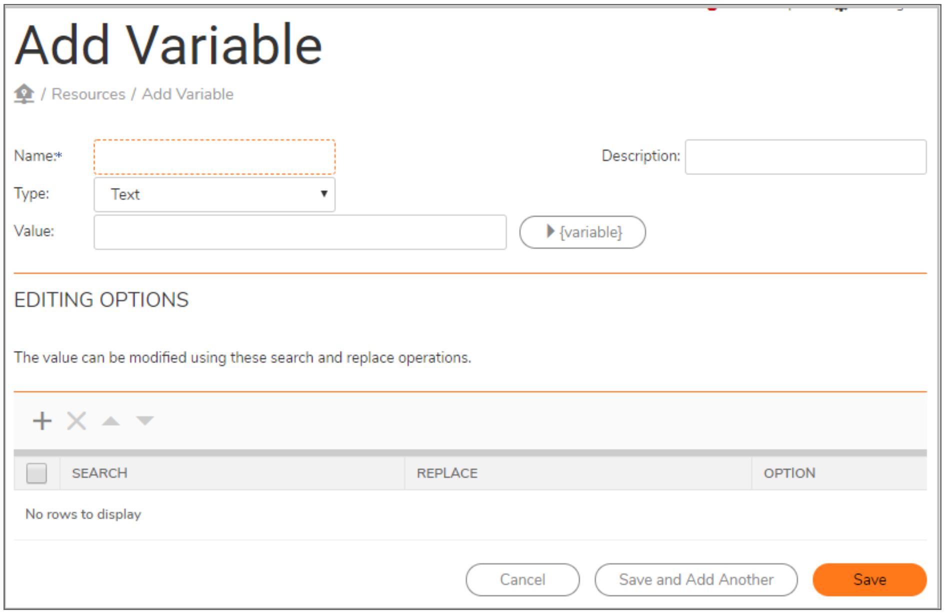
- Creating a Resource Pointing to Users' Remote Desktops
- Creating a WorkPlace Link Giving Users Access to Their Remote Desktops
- Creating a Variable Containing a Variable

Creating a Resource Pointing to Users' Remote Desktops

In order to create a resource that points to users' remote desktops, you need to modify your LDAP store and add an attribute named `rdp`.

To create a resource variable that points to users' remote desktops:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **Variables** tab.
3. Click the **+** (New) icon.


Add Variable

/ Resources / Add Variable

Name:*

Description:

Type: Text

Value:

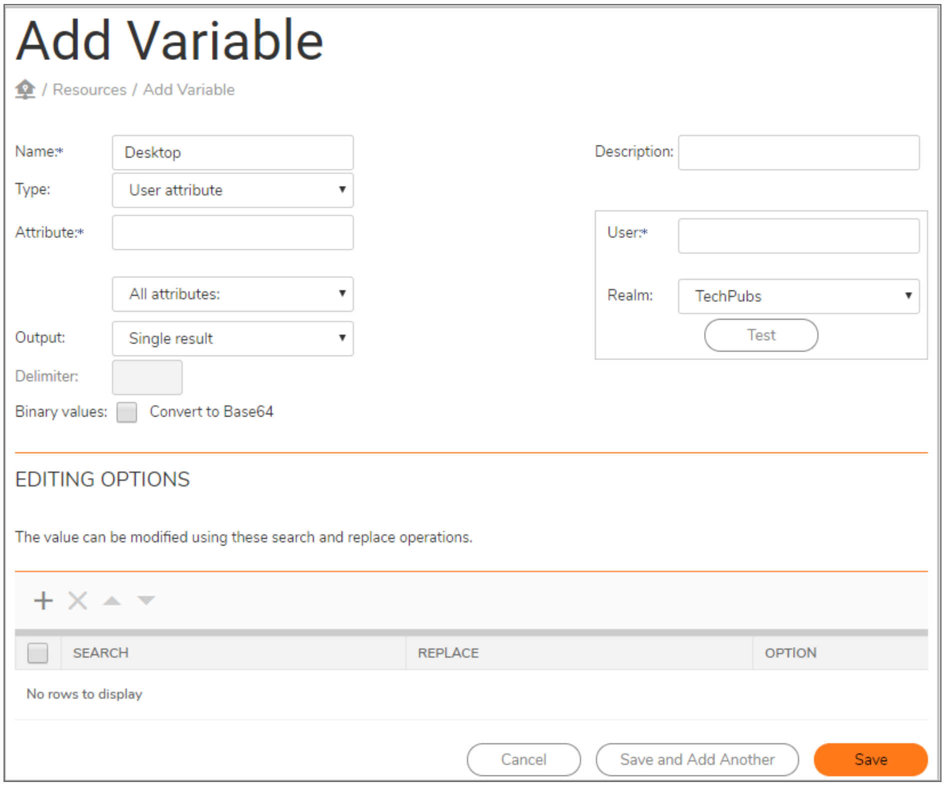
EDITING OPTIONS

The value can be modified using these search and replace operations.

□	SEARCH	REPLACE	OPTION

No rows to display

4. Enter a name for the variable (for example, Desktop), and then select **User attribute** as the **Type.** The options change.


Add Variable

/ Resources / Add Variable

Name:* Desktop

Description:

Type: User attribute

Attribute:*

All attributes:

Output: Single result

Delimiter:

Binary values: □ Convert to Base64

User:*

Realm: TechPubs

EDITING OPTIONS

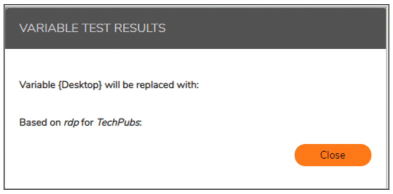
The value can be modified using these search and replace operations.

□	SEARCH	REPLACE	OPTION

No rows to display

5. Enter `rdp` in the **Attribute** field.

6. From the **Output** drop-down menu, leave **Single result** (default) selected if each user has only one computer associated with him or her in the LDAP store.
7. Select the realm to which this new variable applies, and then enter the username of someone who has access to that realm in the **User** field.
8. Click **Test** to make sure that the user attribute you specified returns a value for this user.



Variable {Desktop} will be replaced with:

Based on *rdp* for *TechPubs*:

9. Click **Save**.
10. On the **Resources** tab, click **New**, and then select **Host name or IP**.
11. Give a name to this resource (for example, `Personal computer`).
12. In the **Host name or IP address** field click **{variable}**, and then select *`{Desktop}`*, the variable you created earlier. Click **Insert**.
13. Edit the entry for **Host name or IP address** to add the portion of the address that the personal computers on your network share. The completed entry might look something like this:

    ```
    {Desktop}.dept.company.com
    ```

    As each user logs in, *`{Desktop}`* is replaced by the machine name associated with him or her in the LDAP store using the **rdp** attribute.
14. Click **Save**.

Creating a WorkPlace Link Giving Users Access to Their Remote Desktops

To create a WorkPlace link to give users access to their remote desktops:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **+** (New) icon.
3. Select **Graphical terminal shortcut** from the downdown list.
4. In the **Resource** list, select **Personal computer**, and then specify what the link text will be in WorkPlace. For example, My `remote desktop`.
5. Click **Save**.

   By default, the resource you created will be displayed as a link in WorkPlace titled *My remote desktop*.

When the user John Doe connects to WorkPlace from home or on the road, **{Desktop}** is replaced by the contents of the **rdp** attribute associated with him in the LDAP store, and he sees a WorkPlace link (*My remote desktop*) that points to his office computer (`john_doe-340.dept.company.com`). When Paula Smith follows the same link, she has access to `paula_smith-452.dept.company.com`. If the **rdp** attribute is empty for a given user, then that user will not see a WorkPlace shortcut when he or she logs in.

Creating a Variable Containing a Variable

To create a variable that contains a variable:

You can simplify the creation of user-specific links or shortcuts by using one or more variables to define another one. For example, in the procedure above, a **Host name or IP address** resource was defined as follows, using a variable named **{Desktop}** followed by a string, in this case the path:

```
{Desktop}.dept.company.com
```

You could instead create a variable named **{Desktop_path}** that resolves to the entire path above.

In another example of using multiple variables to create a single variable, you could replace *dept* in the path above with the user's *ou* (organizational unit) attribute in the LDAP store. The below table summarizes the possibilities in the examples outlined here:

AMC Variables

AMC variable name	Resolves to...	Based on...
{Desktop}	*john_doe-340*	*rdp* (LDAP attribute)
{dept}	*Sales*	*ou* (LDAP attribute)
{Desktop_path}	*john_doe-340.dept.company.com*	AMC variable defined as follows: `{Desktop}.dept.company.com`
{Desktop_by_dept}	*john_doe-340.Sales.company.com*	AMC variable defined as follows: `{Desktop}.{ou}.company.com`

Variables cannot be nested more than two deep: you cannot create a variable that refers to a variable that in turn refers to another variable.

Modifying Query Results

You can create a variable by querying an external AD/LDAP store for a specific attribute or set of attributes. To make the query results more useful, you can automatically extract data from them: after the query is sent and the full variable string has been determined, you can perform search and replace operations on its value.

For example, let's say you have a company with offices in multiple locations, and each office uses a different Exchange server for email. Using some editing options, you can define a single variable that represents both Exchange servers, regardless of location.

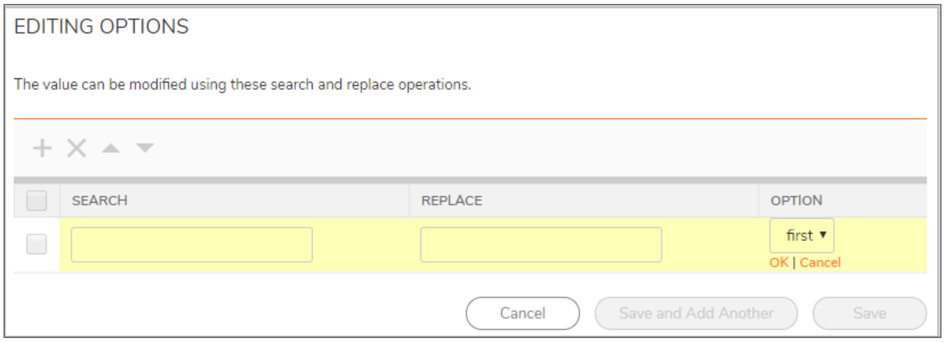
To define a variable by automatically editing the results of a query:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **Variables** tab.
3. Click the **+** (New) icon.
4. In the **Name** field, enter a name for your variable. For example, `Exchange_server`.
5. In the **Type** list, select **User attribute**.

6. Select the appropriate realm from the list: it should point to the AD/LDAP store that you will query.
7. In the **Attribute** list, select **msExchHomeServerName**.
8. Query the directory server for two different employees—for example, one at headquarters in London, and one in California—by entering the user name and clicking **Test** for each one. In this example the only difference is in the server name at the end of the resulting strings:

   ```
   /o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=LN0EXL09
   /o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=CA0EXV08
   ```

9. Modify the query results by clicking the **+** (New) icon in the **Editing options** area:



EDITING OPTIONS

The value can be modified using these search and replace operations.

   a. In the **Search** field, enter:

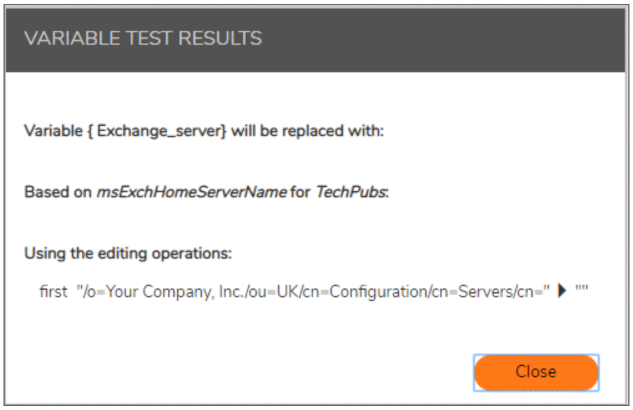
      ```
      /o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=
      ```

   b. Leave the **Replace** field empty, and then click **OK**.

For an employee in the London office or one in California, the variable named **Exchange_server** will contain the appropriate name, either `LN0EXL09` or `CA0EXV08`, depending on the user.

Using the same query, you can create an additional variable that indicates where an employee is based. For example, create a new variable named Location and replace the name of each directory server with its location.

The *Location* variable will resolve to *London* or *California*, depending on the user. For example, when you enter a London employee's name in the **User** field and click **Test**, you'll see the following results:



VARIABLE TEST RESULTS

Variable { Exchange_server} will be replaced with:

Based on *msExchHomeServerName* for *TechPubs*:

Using the editing operations:

first "/o=Your Company, Inc./ou=UK/cn=Configuration/cn=Servers/cn=" ▶ ""

Displaying a Series of Shortcuts Using a Single Definition

When you create a variable based on a user's session properties or the results of a query, the variable can resolve to one value per user attribute (for example, **sAMAccountName** and **lastLogon**), or multiple values (such as a list of groups to which a user belongs, or the workstations a user is permitted to log in to). When a variable can have multiple values, you have the option of creating one shortcut for it that is automatically displayed as a series of shortcuts in WorkPlace.

In this example, we'll create a single shortcut that will result in a series of WorkPlace shortcuts, one for each workstation the user is allowed to access. Here's an overview of the process:

Shortcut Creation Process

Step	Description
A	Create a variable named *User_workstations* that points to a multi-valued attribute in an AD or LDAP server named *userWorkstations*. In the directory store, this attribute lists the workstations a user is allowed to access. For example, a user might have a personal workstation at work, and another workstation that's used for order inventory.
B	Create a host resource named *Workstation_list* that points to the *User_workstations* variable. For the user in this example, the resource has two possible values.
C	Create a WorkPlace graphical terminal shortcut that points to the *Workstation_list* resource. The link for this shortcut will refer to a special, built-in variable named *{URL_REF_VALUE}*, which will automatically result in separate links in WorkPlace for each of the workstations a user is permitted to use.
D	Test WorkPlace. If the shortcut does not appear, it may be because the directory store query is not returning any results. Testing it will also help you see whether you need to adjust the location of the shortcuts in your WorkPlace layout.

A: Create a variable that points to a user attribute in the AD server:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click on the **Variables** tab.
3. Click the **+** (New) icon, and then enter a name for the variable: `User_workstations`.
4. Select **User attribute** in the **Type** list, and then specify the realm that uses the directory store you want to query.
5. In the drop-down menu of attributes returned from the AD store, select *userWorkstations*.
6. In the **Output** list, select *Multiple results*.
7. In the **User** field, enter the name of a representative user (someone who is likely to use this shortcut), and then query the AD/LDAP store for the values of *userWorkstations* by clicking **Test**.
8. The test results will indicate what character (for example, a comma or a semicolon) you should enter in the **Delimiter** field.
9. Click **Save**.

The new variable (*{User_workstations}*) appears in the list and can now be used to define or describe other variables, resources, or WorkPlace shortcuts.

B: Create a host resource that points to the {User_workstations} variable:

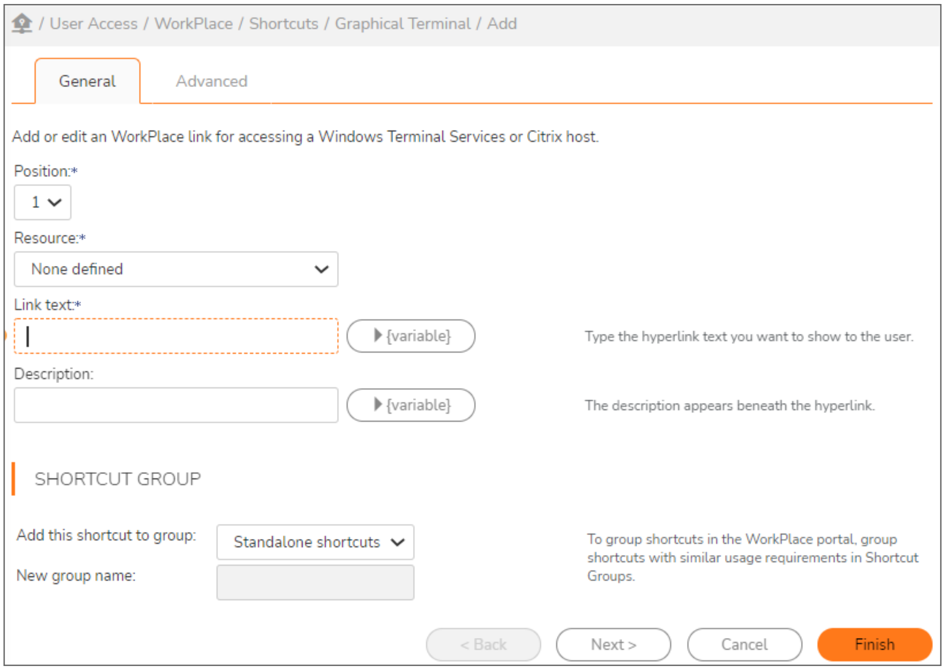
1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon, and then select **Host Name** or **IP Address**.
3. Enter `Workstation_list` as the resource name.
4. In the **Host name or IP address** field, click **{variable}**, and then select **{User_workstations}**, the variable you created in *Step A*.
5. Click **Insert**, and then click **{variable}** again to close the list.
6. Edit the entry for **Host name or IP address** to add the portion of the address that the computers on your network share. The completed entry might look something like this:

   `{User_Workstations}.dept.company.com`

C: Create a WorkPlace shortcut that points to the Workstation_list resource:

1. In the AMC, navigate to **User Access > Workplace**.
2. Click the **Shortcuts** tab.
3. Click the **+** (New) icon.
4. Select **Graphical terminal shortcut** from the drop-down list.

   The **General** tab of the **Add Graphical Terminal Shortcut** page displays.



/ User Access / WorkPlace / Shortcuts / Graphical Terminal / Add
General
Advanced
{variable}
{variable}
< Back
Next >
Cancel
Finish

Add or edit an WorkPlace link for accessing a Windows Terminal Services or Citrix host.

Position:* 1

Resource:* None defined

Link text:*

Type the hyperlink text you want to show to the user.

Description:

The description appears beneath the hyperlink.

SHORTCUT GROUP

Add this shortcut to group: Standalone shortcuts

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

5. In the **Position** field, specify the shortcut's position in the list. The default is **1**. (It's possible to change its position later in your WorkPlace layout.)

6. In the **Resource** drop-down menu, select the resource to which this shortcut will be linked: **Workstation_list**.
7. In the **Link text** field, type the first part of the hyperlink users will see. For example, enter `My workstation(s):` followed by a space.
8. Using a variable you can have the link end in each succeeding value for **Workstation_list**; if there is more than one, then more than one shortcut will be displayed in WorkPlace. Click **{variable}**, and then select **{URL_REF_VALUE}** from the list. Click **Insert** to add the variable to the link text, and then close the list by clicking **{variable}** again. The entry for **Link** now looks like this:

   ```
   My workstation(s): {URL_REF_VALUE}
   ```
9. Click **Finish** to save the shortcut. (For a description of the settings on the **Advanced** page, see Adding Graphical Terminal Shortcuts to Individual Hosts.)

   This shortcut will automatically result in separate links in WorkPlace for each of the workstations a user is permitted to use. The two WorkPlace links in our example—one to a personal workstation and one to a workstation for entering orders—would look like this for the user *ageorge*.

D: Troubleshooting WorkPlace:

1. If users log in to WorkPlace and do not see the shortcut you created, check the following:
   - Is the user in the right community? In the main navigation menu in AMC, click **User Sessions**, and then click the user's name to get session details. The user may not be assigned to the right community, or there may be a rule preventing him or her from accessing the resource.
   - Does the variable return a result for this user? In the main navigation menu in AMC, click **Resources**, and then go to the **Variables** page. Click the variable named `User_workstations`, enter the name of the person who is not seeing the shortcut, and then click **Test**. If no result is returned, the shortcut will not be displayed.
2. Check your WorkPlace layout. When you create a shortcut, you have the opportunity to add it to a group of shortcuts or to the default group (**Standalone shortcuts**). To change the position of the shortcut, click **Realms**, and then click the name of the community to which this user belongs. The WorkPlace Appearance page indicates which layout is being used. To modify page content, click **Manage layouts**.

Creating and Managing Resource Groups

You can define individual resources or manage them in resource groups, which are collections of individual resources. Grouping resources provides a convenient way to manage access to a set of resources with similar characteristics. For example, you might define a resource group containing applications that are important only to your remote employee, simplifying the process of managing access to those resources.

There is no limit to the number of resources that a resource group can contain. When you create a new resource group, it is added to your list of available resources and groups; you can then use the resource group in access control rules.

Topics:

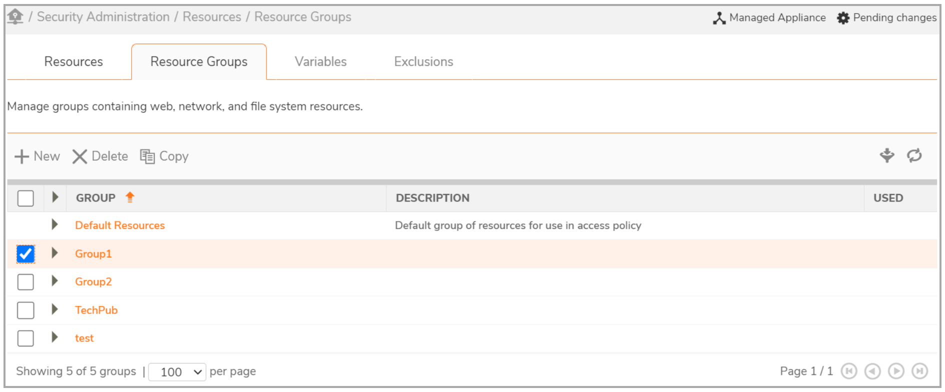
- Adding Resource Groups
- Example: Working with a URL Redirect
- Editing, Deleting and Copying Resource Groups

Adding Resource Groups

When you create a new resource group, it is added to the list of available groups on the **Resource Groups** tab of the **Resources** page.

To add a resource group:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **Resource Groups** tab.

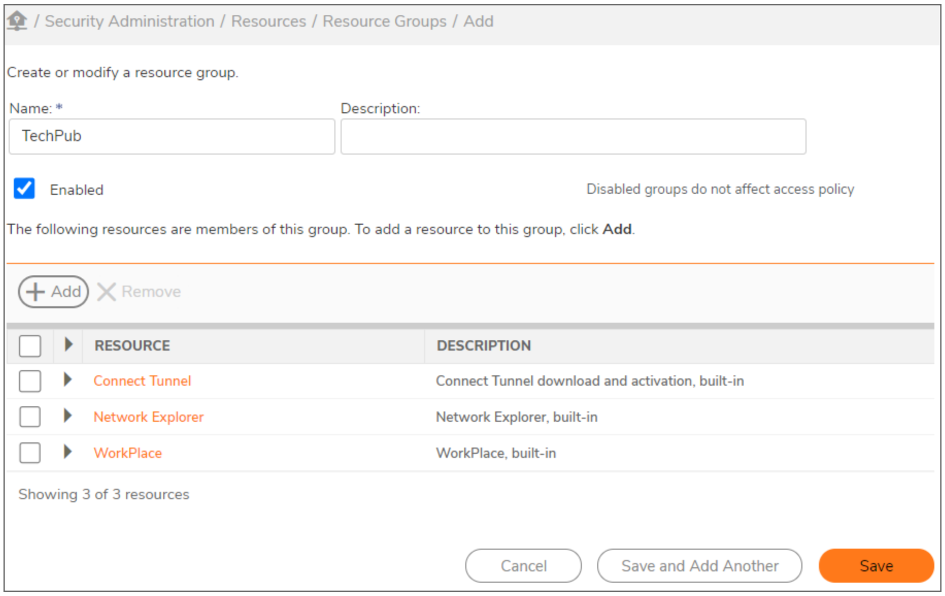


Manage groups containing web, network, and file system resources.

	GROUP	DESCRIPTION	USED
	Default Resources	Default group of resources for use in access policy	
☑	Group1		
□	Group2		
□	TechPub		
□	test		

Showing 5 of 5 groups | 100 per page   Page 1 / 1

3. Click the **+** (New) icon to add a resource group.



/ Security Administration / Resources / Resource Groups / Add

Create or modify a resource group.

Name: * TechPub

Description:

☑ Enabled

Disabled groups do not affect access policy

The following resources are members of this group. To add a resource to this group, click **Add**.

□	RESOURCE	DESCRIPTION
□	Connect Tunnel	Connect Tunnel download and activation, built-in
□	Network Explorer	Network Explorer, built-in
□	WorkPlace	WorkPlace, built-in

Showing 3 of 3 resources

4. Enter a **Name** for the resource group.
5. In the **Description** field, type a descriptive comment about the group.
6. Select the **Enabled** check box to enable the resource group.

   ⓘ | **NOTE:** Disabled resource groups do not allow or deny access.
7. Select the checkbox for each resource you want to include in the group, or leave the group empty and add resources to it later. There is no limit to the number of resources that a group can contain.
8. Click **Save**.

Example: Working with a URL Redirect

Some Web-based applications automatically redirect users to other Web pages. A user accessing the application may browse to a particular Web address, but then be redirected to a different address.

For example, an organization has a mail server with the following URL:

```
http://domino.example.com/dwa.nsf
```

A user who accesses this site is then automatically redirected to a different URL:

```
http://domino.example.com/mail/dwa1.nsf
```

To give users access to the application using the SMA appliance, you need to add both the original and the redirected URLs as resources.

The following example demonstrates how to add your Web-based application as a pair of URL resources, how to group the resources together, and then how to define an access control rule so that your users have access to the application.

Configure URL resources for your Web-based application:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon.
3. Select **URL** from the drop-down list.

   The **Add Resource – URL**page displays.
4. In the **Name** field, type a name for the resource. For example, `Mail Web App`.
5. In the **URL** field, type the address of the mail server. For example,

   `http://domino.example.com/dwa.nsf.`
6. Click **Save**.
7. Repeat *Step 2* through *Step 6* to create a second Web resource specifying the redirected URL address. If your application uses more than one redirected URL, create an additional URL resource for each address; this example assumes there are only two URLs involved.

Create a resource group for both URL resources:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **Resource Groups** tab.
3. Click the **+** (New) icon.

   The **Add Resource Group** page displays.
4. In the **Name** field, type a name for the group resource. For example, `Mail Web App Group`.
5. Select the check boxes for each of the Web resources previously created.
6. Click **Save**.

Define an access control rule for the resource group:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon.

   The **Add Access Rule** page displays.
3. In the **Position** field, type a number to specify the rule's position in the access rule list.
4. Use the **Action** buttons to specify **Permit**.

   This will allow users to access the group resource that you specify in the next step.
5. Complete the information under **Basic settings**:

   a. Leave **User** selected (so that the rule applies to users trying to access a resource).

   b. The **From** field specifies the users to whom the rule applies. For this example, leave the value as **Any user**.

   c. In the **To** field, click **Edit** to specify the target resource for this rule.

      A **Resources** page displays.

   d. Select the resource group previously created. In this example, *Mail Web App Group*.

6. Click **Save**.

For an overview of access control, see Access Control Rules.

Editing, Deleting and Copying Resource Groups

Before modifying a resource group, carefully examine the associated rules to understand how your changes will affect your security policy. You cannot delete a resource group that is referenced in an access control rule. Before deleting a resource group, you must first remove it from any rules in which it is referenced. See Deleting Referenced Objects for more details.

Rather than creating a new resource group from scratch, you can save time by making a copy of an existing group and changing some parameters to fit the new group. Choose a group that shares characteristics with the group you plan to create.

Web Application Profiles

Web application profiles provide single sign-on and translation control for Web applications that use Windows NTLM authentication (v1 and v2 are both supported), or basic authentication.

- With a Web application that uses Windows NTLM authentication, access is granted only to users whose Windows credentials can be verified. Support for NTLM is built into Microsoft IIS (Internet-based services for Windows machines) and supported in all the appliance supported browsers.
- Basic authentication is supported on a wide variety of platforms (note, however, that it sends passwords in the clear across the network).

You can also configure the Web proxy service in AMC to support forms-based authentication, in which users authenticate by filling out a standard HTML form Web using any combination of browser and Web server. Creating Forms-Based Dynamic Single Sign-On Profiles for more information.

Topics:

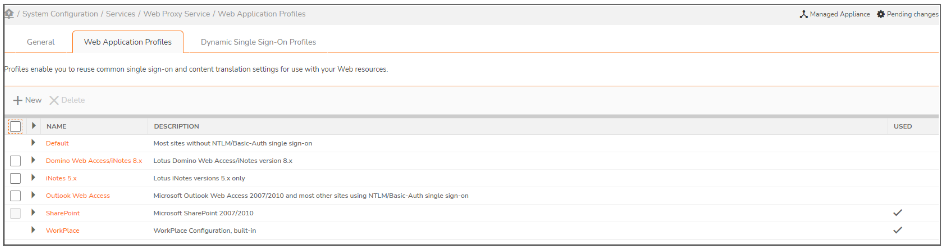
- Viewing Web Application Profiles
- Adding Web Application Profiles
- Preconfigured Web Application Profiles
- Web Application Profile Examples
- Editing and Deleting Web Application Profiles

Viewing Web Application Profiles

Web application profiles are listed on the **Configure Web Proxy Service** page.

To view your list of available Web application profiles:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, click the **Configure** link under **Web proxy service**.
3. To view your available Web profiles, click the **Web Application Profiles** tab.


/ System Configuration / Services / Web Proxy Service / Web Application Profiles
Managed Appliance
Pending changes
General
Web Application Profiles
Dynamic Single Sign-On Profiles
New
Delete

Profiles enable you to reuse common single sign-on and content translation settings for use with your Web resources.

NAME	DESCRIPTION	USED
Default	Most sites without NTLM/Basic-Auth single sign-on	
Domino Web Access/iNotes 8.x	Lotus Domino Web Access/iNotes version 8.x	
iNotes 5.x	Lotus iNotes versions 5.x only	
Outlook Web Access	Microsoft Outlook Web Access 2007/2010 and most other sites using NTLM/Basic-Auth single sign-on	
SharePoint	Microsoft SharePoint 2007/2010	✓
WorkPlace	WorkPlace Configuration, built-in	✓

4. The list includes preconfigured Web application profiles that are recommended for several popular Web applications, any custom Web profiles you created, and a default Web profile. To view the settings for a Web application profile, click its name.

Adding Web Application Profiles

ⓘ **IMPORTANT:** The Web translation that AMC performs is more complete and robust in recent versions of the appliance software.

Web application profiles control single sign-on characteristics, as well as content translation options for a particular Web resource. Each Web resource should have a Web application profile associated with it.

- **Single sign-on** options control whether and how a user’s login credentials are forwarded to downstream Web applications. These options are disabled by default. In addition, one of the following is required to configure single sign-on:
  - Click **Use Web content translation** on the **User Access > WorkPlace > Settings** page in the AMC.
  - Define a WorkPlace link as an aliased URL. This is the approach you should take if you normally redirect traffic through a network agent, but in this case you want to force the resource to be proxied using translated, custom port mapped, or Exchange server FQDN mapped Web access for single sign-on.

  ⓘ **NOTE:** You can configure single sign-on when you create a WorkPlace shortcut for accessing a Windows Terminal Services or Citrix host. See Adding Graphical Terminal Shortcuts to Individual Hosts.
- **Content translation** options control whether hyperlinks in JavaScript code, in cookie bodies, and in cookie paths are translated by the Web proxy service. The options are used only by the translated Web access agent: they are ignored by standard Web access.

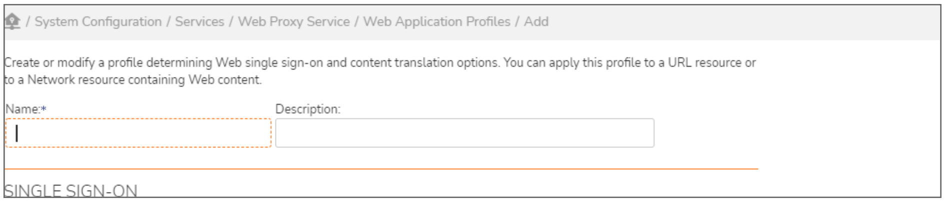
Web application profiles are not used if **Web shortcut access** is set to **Redirect through network agent** on the **Configure WorkPlace** page in AMC.

To add a Web application profile:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, click the **Configure** link under **Web proxy service**.

   The **Web Proxy Service** page displays.
3. Click the **Web Application Profiles** tab.
4. Click the **+** (New) icon.

   The **Add Web Application Profile** page displays.



/ System Configuration / Services / Web Proxy Service / Web Application Profiles / Add

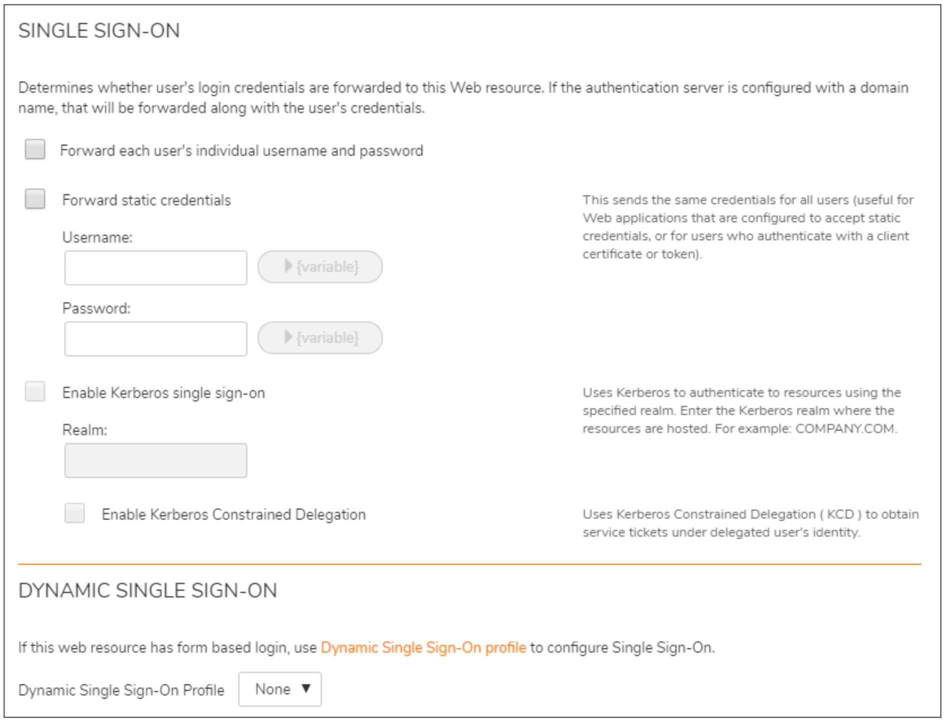
Create or modify a profile determining Web single sign-on and content translation options. You can apply this profile to a URL resource or to a Network resource containing Web content.

Name:*

Description:

SINGLE SIGN-ON

5. In the **Name** field, type a name for the profile. If you are creating a profile to associate with a specific application, you might want to give it a name similar to that of the application.
6. In the **Description** field, type a descriptive comment about the profile.
7. In the **Single Sign-On** area, specify if and how you want user credentials to be passed along to the Web resource. Forwarding user credentials prevents the user from having to log in multiple times (once to get to the appliance, and again to access an application resource).



SINGLE SIGN-ON

Determines whether user's login credentials are forwarded to this Web resource. If the authentication server is configured with a domain name, that will be forwarded along with the user's credentials.

☐ Forward each user's individual username and password

☐ Forward static credentials

This sends the same credentials for all users (useful for Web applications that are configured to accept static credentials, or for users who authenticate with a client certificate or token).

Username:

Password:

☐ Enable Kerberos single sign-on

Uses Kerberos to authenticate to resources using the specified realm. Enter the Kerberos realm where the resources are hosted. For example: COMPANY.COM.

Realm:

☐ Enable Kerberos Constrained Delegation

Uses Kerberos Constrained Delegation (KCD) to obtain service tickets under delegated user's identity.

DYNAMIC SINGLE SIGN-ON

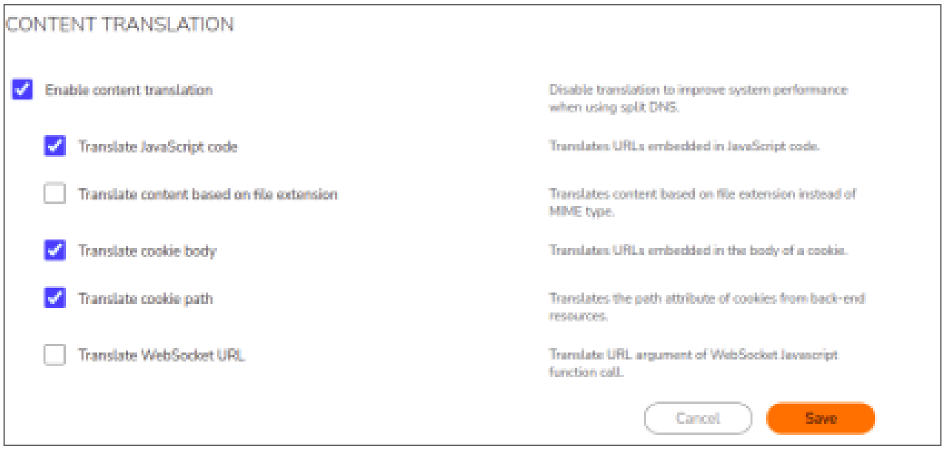
If this web resource has form based login, use Dynamic Single Sign-On profile to configure Single Sign-On.

Dynamic Single Sign-On Profile: None ▼

- If you select the **Forward each user's individual username and password** check box, the username and password used to authenticate to WorkPlace are forwarded to the back-end Web server.
- If you select the **Forward static credentials** check box, the appliance forwards the same username and password for all users. This is useful for Web sites that require HTTP basic authentication, but don't provide personalized content for each user based on the login name. It's also useful for users who authenticate with a client certificate or token.
- If you do not select either option, single sign-on functionality is disabled. If you select both options, the individual username and password option takes precedence. For example, if the user provides a username/password pair, it is forwarded, but if username/password is not provided, the Web proxy service forwards the static credentials.
- If you select the **Enable Kerberos single sign-on** check box and specify the Kerberos realm where the resources are hosted, WorkPlace and Connect Tunnel users can access http resources. This realm is used for authenticating environments like Active Directory, Active Directory Tree, and Active Directory Forest where Kerberos is configured as a preferred authentication mechanism.

8. In the **Dynamic Single Sign-On** area, configure the Dynamic Single Sign-On profile or select from the drop-down. For more information on how to configure, see Creating Forms-Based Dynamic Single Sign-On Profiles.
9. In the **Content translation** area, select the **Enable Content translation** check box and items that you want the Web proxy service to translate.

ⓘ **NOTE:** The **Enable Content translation** check box is enabled by default for both new installation and upgrade or import.



CONTENT TRANSLATION

☑ Enable content translation — Disable translation to improve system performance when using split DNS.

☑ Translate JavaScript code — Translates URLs embedded in JavaScript code.

□ Translate content based on file extension — Translates content based on file extension instead of MIME type.

☑ Translate cookie body — Translates URLs embedded in the body of a cookie.

☑ Translate cookie path — Translates the path attribute of cookies from back-end resources.

□ Translate WebSocket URL — Translate URL argument of WebSocket Javascript function call.

- Ensure the **Enable Content translation** check box is clear if you want to disable URL translation for URL resources using split Domain Name System (DNS) approach. When configuring a URL resource, if both the resource's Fully Qualified Doamain Name (FQDN) and the appliance's FQDN for that resource are the same, then there is no need for translation. In such cases, you can disable URL translation to improve the system performance.
- Select the **Translate JavaScript code** check box if you want the Web proxy service to translate links embedded in JavaScript code used by the Web resource. This is useful for JavaScript that

contains absolute URLs or absolute references (`/to/path/xyz`), or that dynamically generates URLs (for example, `location="http://" + host name + "/index.html"`). This improves compatibility with Microsoft Outlook Web Access and other applications that rely on JavaScript. This option is enabled by default.

However, if you notice problems with searching mail based on the Subject, From, or Sent To fields, or if you see an error after logging in when you access OWA using a WorkPlace shortcut, clear the **Translate JavaScript code** check box for the OWA profile.

- Select the **Translate content based on file extension** check box if you want the Web proxy service to determine content type by examining the file extension, not the MIME type. Normally, the Web proxy service translates certain content types (including text and HTML). It determines the content type from the MIME type in the HTTP header. If a Web resource is sending the incorrect MIME type, select this option and the Web proxy service will decide whether or not to translate a file based on its file extension. This option is disabled by default.
- Select the **Translate cookie body** check box if you want the Web proxy service to translate URLs embedded in the body of a cookie. If a Web resource uses embedded URLs in the body of a cookie (which is not common practice), and you do not have this option enabled, users can experience problems. A common symptom is being unexpectedly redirected to another URL. This option is enabled by default.
- Select the **Translate cookie path** check box if you want the Web proxy service to translate the path attribute of cookies sent by back-end resources. The browser uses cookie paths to determine when to send a cookie back to the server. The appliance changes the path that the browser sees, so if the cookie path is not translated, the browser will never send the cookie. A common symptom of this situation is a user being prompted repeatedly for login credentials after already entering valid ones. If this occurs, you should enable this option. This option is enabled by default.
- Select the **Translate WebSocket URL** check box if you want the Web proxy service to translate URL argument of WebSocket Javascript function calls. Selecting this option enables SMA to support all the HTML WebSocket based applications.

10. Click **Save**.

Preconfigured Web Application Profiles

Several preconfigured Web application profiles are included with the appliance and are recommended for certain commonly used Web applications. (More can be added; see Adding Web Application Profiles.) Preconfigured profiles are shown in the below table.

Preconfigured Web Application Profiles

Web application profile	Description
Default	A default profile that you can use for most Web applications or sites that don’t use NTLM or basic authentication single sign-on
Domino Web Access / iNotes 8.x	A profile for Lotus Domino Web Access (versions 8.x only)
iNotes 5.x	A profile for Lotus iNotes (versions 5.x only)
Outlook Web Access	A profile for Microsoft Outlook Web Access and other sites that use NTLM or basic authentication single sign-on

SharePoint	A profile for SharePoint
WorkPlace	A read-only profile for WorkPlace

Web Application Profile Examples

This section explains how the appliance determines which Web application profile to apply to an incoming request, and demonstrates the flexibility of using profiles when specifying resources.

Topics:

- How Requests for Web Resources are Evaluated
- Associating one profile with an entire domain

How Requests for Web Resources are Evaluated

Because Web resources can be defined quite broadly, the appliance follows a rule for determining which Web application profile to apply to an incoming request: it chooses the profile associated with the most specific resource.

For example, suppose you've defined these two resources:

- A DNS domain (`xyz.com`) with `Web application profile A` attached
- A specific Web server (`web1.xyz.com`) with `Web application profile B` attached

If a user request comes in for ***https://web1.xyz.com/timesheet.html***, the appliance uses `Web application profile B` because it is associated with a more specific resource (the Web server) than `Web application profile A` (the domain). The actual order that the appliance uses is as follows:

URL —> Host name —> IP address —> Subnet/IP range —> DNS domain

Associating one profile with an entire domain

If you want to associate the same Web application profile to all resources within a single domain, associate a profile with that domain, and then select *None* as the profile for any individual resources you define that are within that domain. The individual resource will inherit the domain's profile. If there is no profile associated with a particular resource, and there is no profile to inherit, the appliance uses the system defaults for the profile.

Editing and Deleting Web Application Profiles

Before modifying a profile, confirm that the changes will be compatible with its associated applications.

If a profile is still associated with one or more resources, AMC prevents you from deleting it. You must remove all associations before you can delete the profile. See Deleting Referenced Objects for more details.

Configuring a Single Sign-On Authentication Server

Single sign-on (SSO) allows you to configure the appliance to forward user credentials to back-end Web resources. It also means that the user does not need to log in multiple times (once to get to the appliance, and again to access an application resource).

The appliance supports various types of Web SSO (as a security measure, SSO is disabled by default).

ⓘ | **NOTE:**

- To use SSO functionality when accessing Web applications during tunnel sessions, you can enable **Web resource filtering**. See Configuring Web Resource Filtering for more information.
- By default, Web content is proxied directly through the appliance for users running OnDemand Tunnel. Select **Use Web content translation** in the **Web shortcut access** area of the **Configure WorkPlace** page in AMC.

Topics:

- Forms-Based Single Sign-On
- Basic Authentication Forwarding
- NTLM Authentication Forwarding

Forms-Based Single Sign-On

Many Web applications use forms-based authentication, where the user interface for authentication is a Web form. You can use AMC to set up a single sign-on profile that will forward a user's appliance credentials to a Web application that uses forms-based authentication. There are some built-in profiles that you can modify for your environment:

- OWA (multiple versions)
- SharePoint

ⓘ | **NOTE:** Forms-based SSO is supported only with translation. For other access agents (Web proxy and OD Tunnel) access the backend Web application cookies required for translation are not provisioned to the server.

Creating Forms-Based Dynamic Single Sign-On Profiles

Legacy Single Sign-On profile supports SSO authentication for applications such as OWA, Citrix ZenApp, and Citrix ZenDesktop. To overcome this limitation and to support all the third party applications such as Confluence, Jira, SonicWall Firewall, and so on, SMA is enhanced to support Dynamic Single Sign-On profile which allows SSO authentication on any type of resources.

ⓘ | **NOTE:** Legacy SSO is deprecated and enhanced with Dynamic Single Sign On feature. If you wish to use the Legacy SSO, you can still use by enabling the CEM setting to `AMC_SHOW_LEGACY_SSO_PROFILES=true`.

See Creating Forms-Based Dynamic Single Sign-On Profiles for more information.

Basic Authentication Forwarding

This form of authentication forwarding is supported on a wide variety of platforms, but is not very secure because it sends passwords in the clear across the network. The appliance can be configured to send each user’s authentication credentials, or “static” credentials (that is, the same credentials for all users).

To configure basic authentication forwarding:

1. Configure a Web application profile to use SSO and specify which user credentials to use.
2. Attach the Web application profile to any Web resources for which you want to use SSO.

Basic authentication forwarding is configured within a Web application profile. For more information, see Adding Web Application Profiles.

NTLM Authentication Forwarding

NTLM (Windows NT LAN Manager) uses a challenge/response mechanism to securely authenticate users without sending passwords in the clear across the network. It provides a secure method for sending Windows network credentials to a Microsoft IIS (Internet Information Services) Web server.

NTLM authentication forwarding passes a Windows domain name along with the user's authentication credentials. This enables users accessing Web resources on Windows networks to be securely authenticated without sending their passwords in the clear.

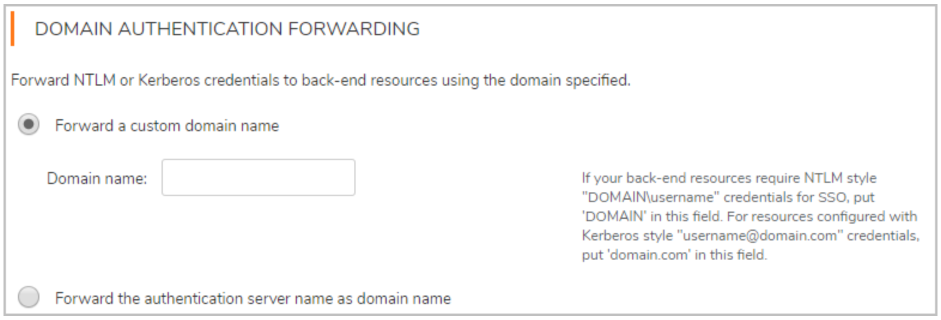
ⓘ | **NOTE:**

- To use NTLM authentication forwarding in situations in which the credentials do not match, users must be running a Web browser that supports NTLM.
- When single sign-on is enabled, the Web proxy service and the back-end server determine which authentication method is used. If only one authentication method (basic authentication or NTLM authentication) is enabled in AMC, that method is used. However, if both methods are enabled in AMC, NTLM authentication is used because it is the more secure of the two.

To configure NTLM authentication forwarding:

1. Enable the SSO options in a Web application profile, and then attach the profile to any Web resources to which you want to forward user credentials.
2. In the AMC, navigate to **System Configuration > Authentication Servers**.
3. Click the **Edit** link for the server you want to configure.

   The **Configure Authentication Server** page displays.
4. Expand the **Advanced** settings.
5. Specify the domain name you want to forward in the **Domain authentication forwarding** area:



DOMAIN AUTHENTICATION FORWARDING

Forward NTLM or Kerberos credentials to back-end resources using the domain specified.

● Forward a custom domain name

Domain name:

If your back-end resources require NTLM style "DOMAIN\username" credentials for SSO, put 'DOMAIN' in this field. For resources configured with Kerberos style "username@domain.com" credentials, put 'domain.com' in this field.

○ Forward the authentication server name as domain name

- You can type a custom name in the **Domain name** field, but it is not required. If you do not specify a name, an empty (null) domain name is forwarded, along with the user credentials.
- To forward the authentication server **name** (as specified in the Name field at the top of the page) along with the user credentials, click **Forward the authentication server name as domain name**.

Creating Forms-Based Dynamic Single Sign-On Profiles

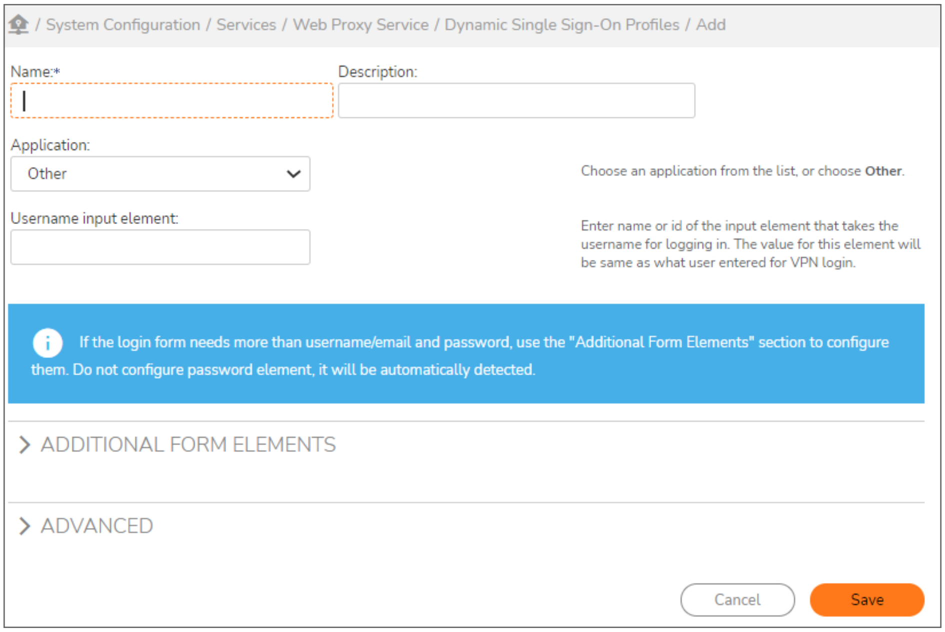
Use AMC to set up a single sign-on profile that will forward a user's appliance credentials to a Web application that uses forms-based authentication.

To create a form based dynamic single sign-on profile:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, click the **Configure** link under **Web proxy service**.

   The **Web Proxy Service** page displays.
3. Click the **Dynamic Single Sign-On Profiles** tab.
4. Click the + (New) icon.

   The **Dynamic Single Sign-On Profile** page displays.



/ System Configuration / Services / Web Proxy Service / Dynamic Single Sign-On Profiles / Add

Name:*

Description:

Application: Other

Choose an application from the list, or choose **Other**.

Username input element:

Enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user entered for VPN login.

If the login form needs more than username/email and password, use the "Additional Form Elements" section to configure them. Do not configure password element, it will be automatically detected.

   a. Type a **Name** and **Description**.

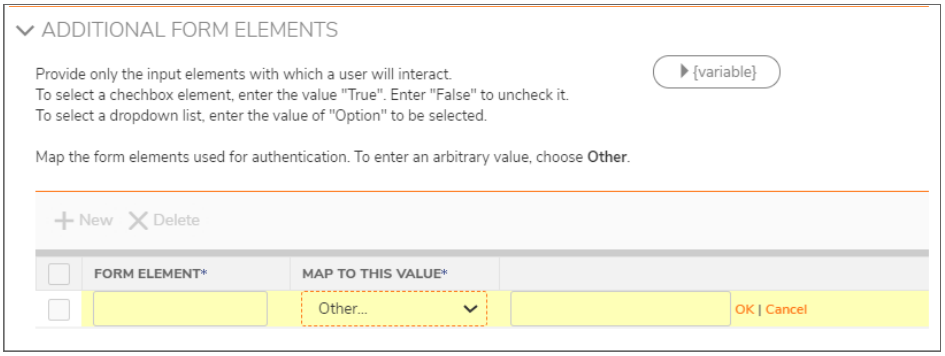
   b. Select the applicable application from the **Application** list. (To start from scratch and specify elements from a custom form, select **Other**).

   c. In the **Username input element** field, enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user need to enter for

VPN login.

ⓘ **NOTE:** If the login form needs more than username/email and password, use the "**Additional Form Elements**" section to configure them.
Do not configure password element, it will be automatically detected.

5. In the **Additional Form Elements** section, click the + icon.



Provide only the input elements with which a user will interact.
To select a chechbox element, enter the value "True". Enter "False" to uncheck it.
To select a dropdown list, enter the value of "Option" to be selected.

Map the form elements used for authentication. To enter an arbitrary value, choose **Other**.

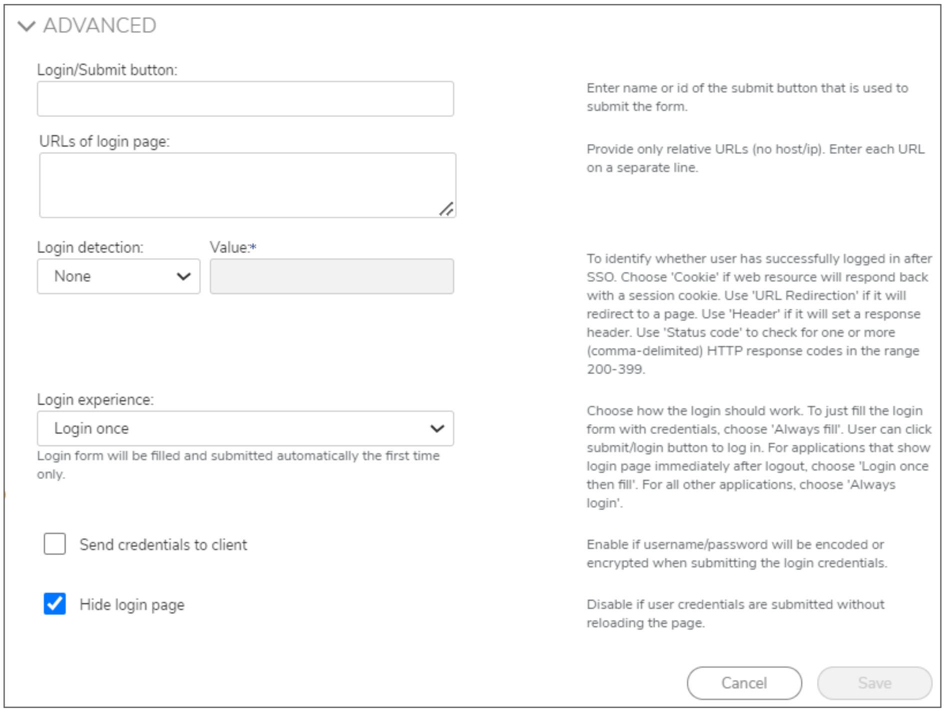
□	FORM ELEMENT*	MAP TO THIS VALUE*	
□		Other...	

   a. In the **Form Element** field, enter the input element with which an user will interact.

   b. In the **Map To This Value** drop-down, select the value for which the form element to be mapped.

   c. Click **OK**.

6. In the **Advanced** section, enter name or id of the submit button that is used to submit the form in the **Login /Submit button** field.



Login/Submit button:

Enter name or id of the submit button that is used to submit the form.

URLs of login page:

Provide only relative URLs (no host/ip). Enter each URL on a separate line.

Login detection: None

Value:*

To identify whether user has successfully logged in after SSO. Choose 'Cookie' if web resource will respond back with a session cookie. Use 'URL Redirection' if it will redirect to a page. Use 'Header' if it will set a response header. Use 'Status code' to check for one or more (comma-delimited) HTTP response codes in the range 200-399.

Login experience: Login once

Login form will be filled and submitted automatically the first time only.

Choose how the login should work. To just fill the login form with credentials, choose 'Always fill'. User can click submit/login button to log in. For applications that show login page immediately after logout, choose 'Login once then fill'. For all other applications, choose 'Always login'.

□ Send credentials to client

Enable if username/password will be encoded or encrypted when submitting the login credentials.

☑ Hide login page

Disable if user credentials are submitted without reloading the page.

ⓘ **NOTE:** The **Submit** field is optional. When not configured it is automatically detected. Leave this field empty and update it only when auto-detect is not correctly identifying it.

a. In the **URLs of login page** field, enter the relative URLs without host or IP address. Enter each URL in a separate line.

   ⓘ **NOTE:** The **URLs of login page** field is optional and can be left empty. Use it only when auto-detection of login page fails.

b. In the **Login detection** drop-down, select the detection option of the URL and enter the respective value.

   - **Cookie**- Select this option only if the web application sets a cookie when the login is successful. Set the value as name of the cookie. Example: JSESSIONID
   - **URL Redirection**- Select this option only if the web application redirects the user to a different page on successful login. Set the value as partial URL that will match the redirected URL. Example: /home.action
   - **Header**-Select this option only if the web application sets a response header on successful login. Set the value as name of the response header. Example: X-Session-Id
   - **Status code**-Select this option only if the web application sends a distinct HTTP status code as response to login request. Set the value as HTTP status code. Multiple values can be configured using comma as delimiter.

c. In the **Login experience** drop-down, allows you to specify when the user will be automatically logged into the web application Select the following login form behavior based on the resource application:

   - **Always login (fill and submit)** to fill and submit the login form automatically every time. Suitable for most applications. Do not use if application shows login page immediately after logging out.
   - **Always fill (but do not submit)** to fill the login form with credentials every time the login page is shown to the user. But the login form will not be submitted automatically. User can manually click the login/submit button if they intend to login.
   - **Login once then fill** to fill and submit the login form automatically the first time. If the login page is shown after logging out of the application, login form will filled with credentials but not submitted automatically. User can manually click login/submit button to login if needed. Suitable for application showing login page immediately after logging out.
   - **Login once** to fill and submit the login form automatically the first time only. Subsequent login page will not be automatically logged in or filled.

7. Select **Send credentials to client** check box if username/password is encoded or encrypted by web application when submitting the login credentials.
8. Unselect the **Hide login page** check box if user credentials need to submitted without reloading the page.
9. Click **Save**.

Assign this Dynamic Single Sign-On Profile to appropriate Web Application Profile of a resource. When configured, user’s credentials are automatically sent to the back-end server when the user reaches login page and user gets automatically logged in.

For information on configuring SSO for a Web application that uses Windows NTLM or basic authentication, see Web Application Profiles.

Dynamic SSO Profile for Microsoft RDWeb

Microsoft Remote Desktop Web Access (Microsoft RD Web Access) is a Remote Desktop Service role that allows users to access RemoteApp and Desktop connection through the start menu or a web browser.

From 12.4.2 onwards, you can quickly configure Single Sign-On for Microsoft RDWeb service by selecting **Microsoft Remote Desktop Web Client** option while creating a Dynamic Single Sign-On profile.

Topics:

- Configuring Microsoft RD Web Access in AMC

Configuring Microsoft RD Web Access in AMC

After you complete the configurations you can access RemoteApp and Desktop connection without the need to manually login.

Topics:

- Creating Dynamic SSO Profile for Microsoft Remote Desktop Web Client
- Creating Web Application Profile
- Creating RDWeb URL resource with custom access
- Adding RDWeb in start page

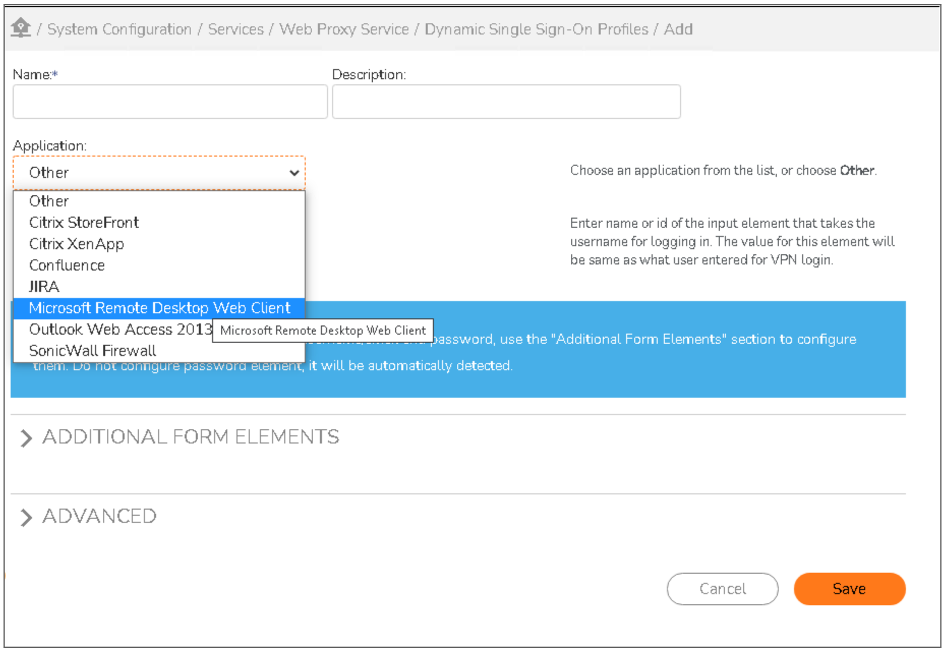
Creating Dynamic SSO Profile for Microsoft Remote Desktop Web Client

To create a form based dynamic single sign-on profile:

1. In the AMC, navigate to **System Configuration** > **Services**.
2. In the **Access Services** section, click the **Configure** under **Web proxy service**.

   The **Web Proxy Service** page displays.
3. Click the **Dynamic Single Sign-On Profiles** tab.
4. Click the + (New) icon.

   The **Dynamic Single Sign-On Profile** page displays.
5. Type a **Name** and **Description**.
6. Select **Microsoft Remote Desktop Web Client** from the **Application** list.



/ System Configuration / Services / Web Proxy Service / Dynamic Single Sign-On Profiles / Add

Name:*

Description:

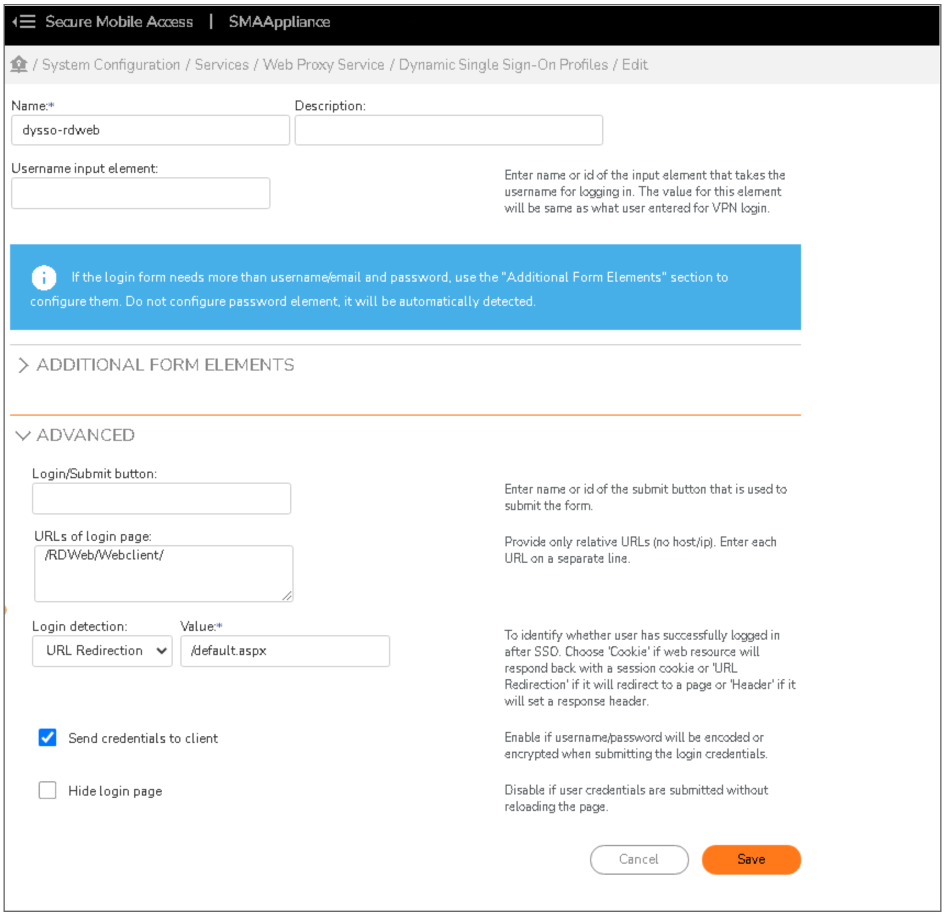
Application: Other

Choose an application from the list, or choose Other.

Enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user entered for VPN login.

password, use the "Additional Form Elements" section to configure them. Do not configure password element, it will be automatically detected.

ⓘ **NOTE:** Selecting Microsoft Remote Desktop Web Client from the Application list loads the pre-configured system profile for MS RDWeb.



Secure Mobile Access | SMAAppliance

/ System Configuration / Services / Web Proxy Service / Dynamic Single Sign-On Profiles / Edit

Name:* dysso-rdweb

Description:

Username input element:

Enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user entered for VPN login.

If the login form needs more than username/email and password, use the "Additional Form Elements" section to configure them. Do not configure password element, it will be automatically detected.

> ADDITIONAL FORM ELEMENTS

ADVANCED

Login/Submit button:

Enter name or id of the submit button that is used to submit the form.

URLs of login page: /RDWeb/Webclient/

Provide only relative URLs (no host/ip). Enter each URL on a separate line.

Login detection: URL Redirection

Value:* /default.aspx

To identify whether user has successfully logged in after SSO. Choose 'Cookie' if web resource will respond back with a session cookie or 'URL Redirection' if it will redirect to a page or 'Header' if it will set a response header.

☑ Send credentials to client

Enable if username/password will be encoded or encrypted when submitting the login credentials.

☐ Hide login page

Disable if user credentials are submitted without reloading the page.

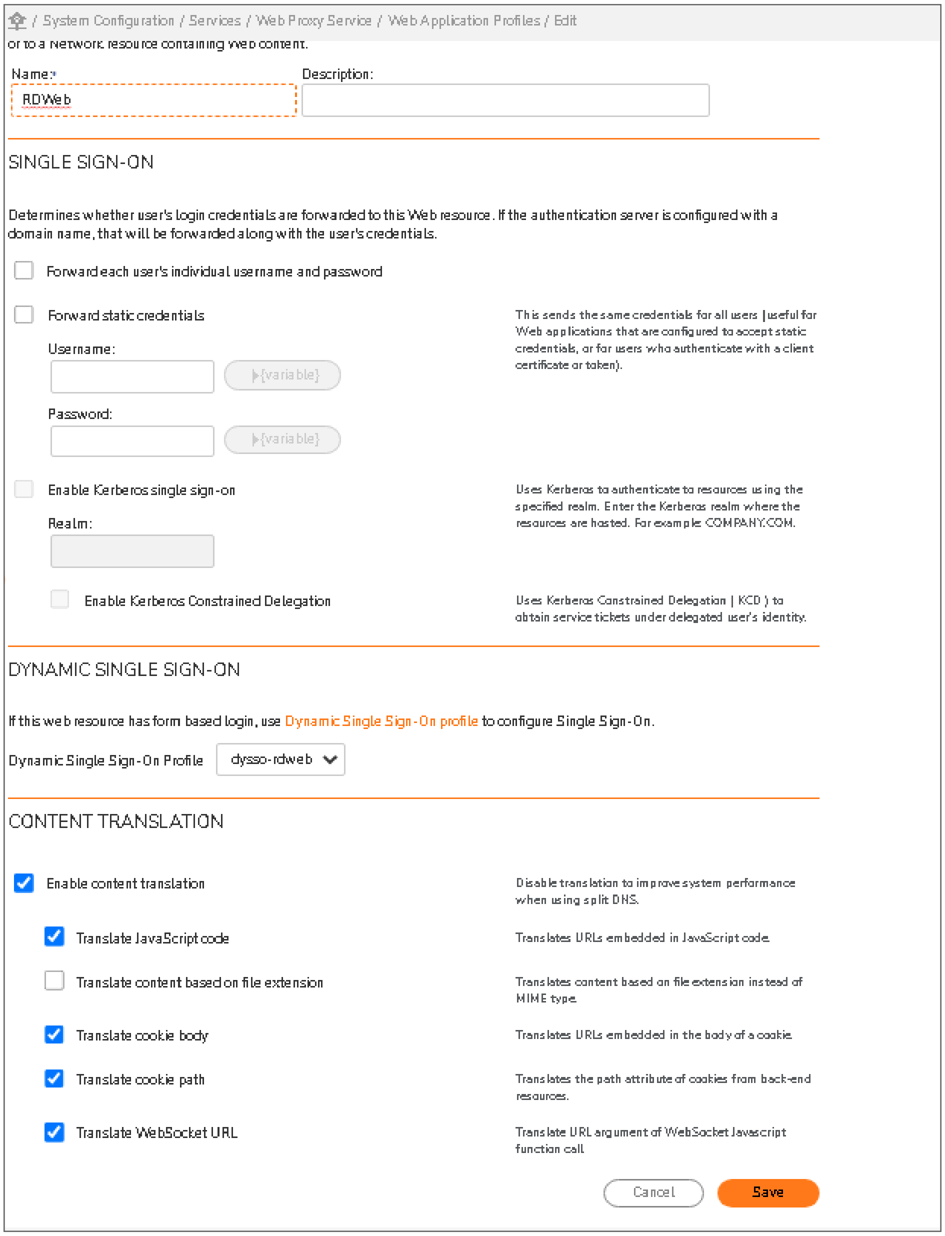
7. Click **Save**.

Creating Web Application Profile

1. In the AMC, navigate to **System Configuration** > **Services**.
2. In the **Access Services** section, click the **Configure** under **Web proxy service**.

   The **Web Proxy Service** page displays.
3. Click the **Web Application Profiles** tab.
4. Click the + (New) icon.

   The **Add Web Application Profile** page displays.
5. Enter the name and description.
6. Configure **Dynamic Single Sign-On** by adding the above created RDWeb Dynamic SSO profile.
7. Under **Content translation**, select the **Translate WebSocket URL**check box.



/ System Configuration / Services / Web Proxy Service / Web Application Profiles / Edit

or to a network resource containing web content.

Name:* RDWeb

Description:

SINGLE SIGN-ON

Determines whether user's login credentials are forwarded to this Web resource. If the authentication server is configured with a domain name, that will be forwarded along with the user's credentials.

□ Forward each user's individual username and password

□ Forward static credentials — This sends the same credentials for all users (useful for Web applications that are configured to accept static credentials, or for users who authenticate with a client certificate or token).

Username: {variable}

Password: {variable}

□ Enable Kerberos single sign-on — Uses Kerberos to authenticate to resources using the specified realm. Enter the Kerberos realm where the resources are hosted. For example COMPANY.COM.

Realm:

□ Enable Kerberos Constrained Delegation — Uses Kerberos Constrained Delegation (KCD) to obtain service tickets under delegated user's identity.

DYNAMIC SINGLE SIGN-ON

If this web resource has form based login, use Dynamic Single Sign-On profile to configure Single Sign-On.

Dynamic Single Sign-On Profile: dysso-rdweb

CONTENT TRANSLATION

☑ Enable content translation — Disable translation to improve system performance when using split DNS.

☑ Translate JavaScript code — Translates URLs embedded in JavaScript code.

□ Translate content based on file extension — Translates content based on file extension instead of MIME type.

☑ Translate cookie body — Translates URLs embedded in the body of a cookie.

☑ Translate cookie path — Translates the path attribute of cookies from back-end resources.

☑ Translate WebSocket URL — Translate URL argument of WebSocket Javascript function call

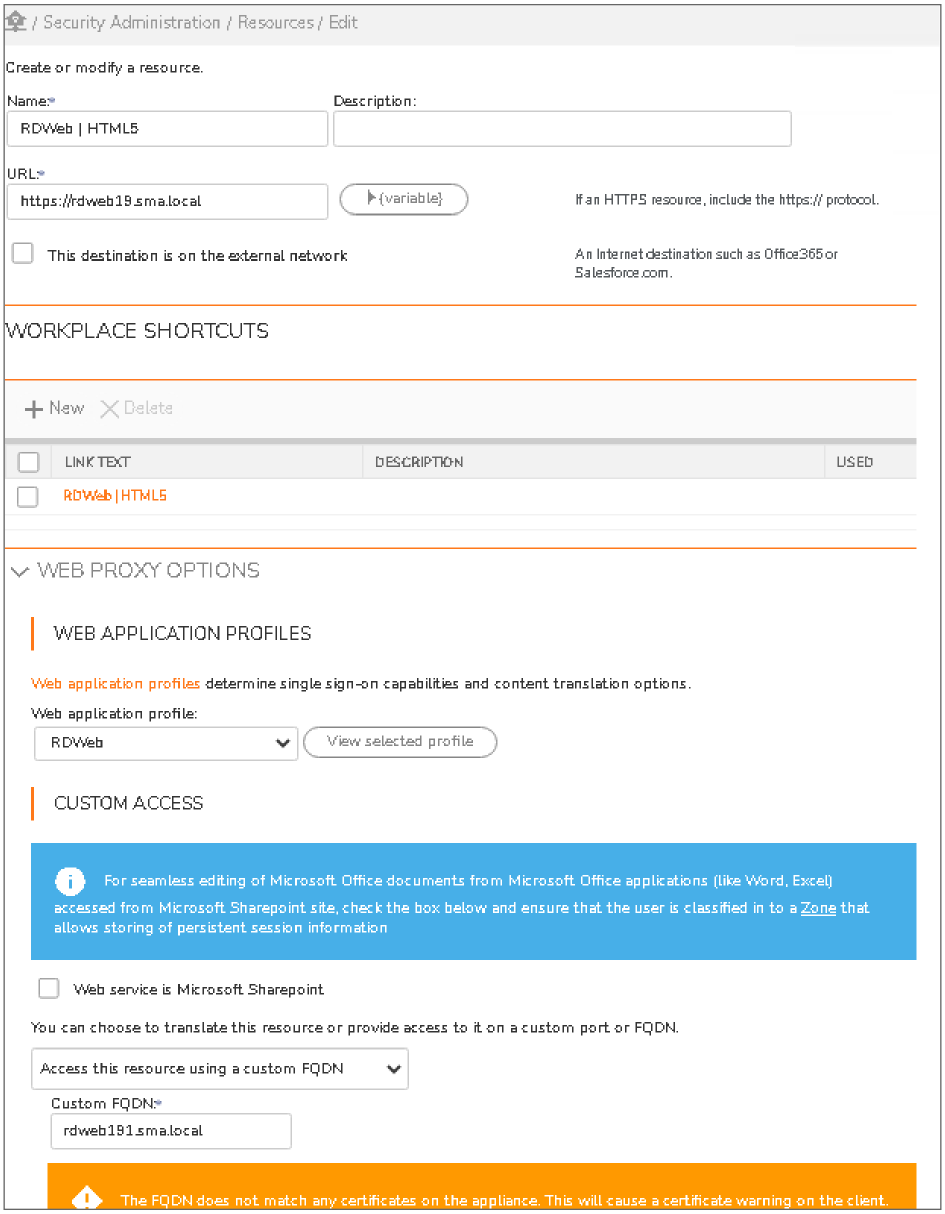
8. Click **Save**.

Creating RDWeb URL resource with custom access

1. In the AMC, navigate to **Security Administration** > **Resources**.
2. Click the + (New) icon.
3. Select URL from the drop-down list.

   The **Add Resource - URL** page displays.

4. In the **Name** field, enter the name for this URL resource.
5. In the **URL** field, enter the URL.
6. Select the **Create Shortcut on WorkPlace** check box.
7. Expand **Web Proxy Options** and do the following:
    a. Under **Web Application profile**, select the created web application profile.
    b. Under **Custom Access** section, select **Access this resource using a custom FQDN**.
    c. Provide **Custom FQDN**.



/ Security Administration / Resources / Edit

Create or modify a resource.

Name: RDWeb | HTML5

Description:

URL: https://rdweb19.sma.local

If an HTTPS resource, include the https:// protocol.

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUTS

□	LINK TEXT	DESCRIPTION	USED
□	RDWeb | HTML5		

WEB PROXY OPTIONS

WEB APPLICATION PROFILES

Web application profiles determine single sign-on capabilities and content translation options.

Web application profile: RDWeb

CUSTOM ACCESS

For seamless editing of Microsoft Office documents from Microsoft Office applications (like Word, Excel) accessed from Microsoft Sharepoint site, check the box below and ensure that the user is classified in to a Zone that allows storing of persistent session information

□ Web service is Microsoft Sharepoint

You can choose to translate this resource or provide access to it on a custom port or FQDN.

Access this resource using a custom FQDN

Custom FQDN: rdweb191.sma.local

The FQDN does not match any certificates on the appliance. This will cause a certificate warning on the client.

8. Click **Save**.

Adding RDWeb in start page

1. In the AMC, navigate to User Access > Workplace.
2. Click the Shortcuts tab.
3. Select **RDWeb**.
4. Click **Next** to display the **Advanced** page.
5. Select the **All devices** check box.
6. In the **Start page** field, enter URL `/RDWeb/webclient/`.
7. Click **Save**.

Dynamic SSO Profile for Citrix XenApp

Citrix XenApp is an application virtualization service that provides ondemand Windows-based applications to devices and works in the context of the Citrix XenDesktop desktop virtualization service.

From 12.4.2 onwards, you can quickly configure Single Sign-On for Citrix XenApp service by selecting **Citrix XenApp** option while creating a Dynamic Single Sign-On profile.

Topics:

- Configuring Citrix XenApp in AMC

Configuring Citrix XenApp in AMC

After you complete the configurations you can access Citrix XenApp and Desktop connection without the need to manually login.

Topics:

- Creating Dynamic SSO Profile for Citrix XenApp
- Creating Web Application Profile
- Creating Citrix XenApp URL resource with custom access
- Adding Citrix Xenapp in start page

Creating Dynamic SSO Profile for Citrix XenApp

To create a form based dynamic single sign-on profile:

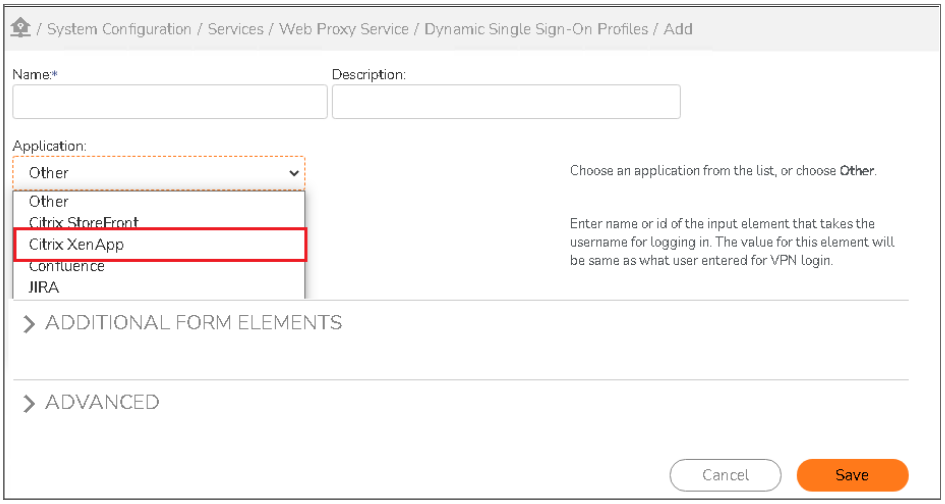
1. In the AMC, navigate to **System Configuration** > **Services**.
2. In the **Access Services** section, click the **Configure** under **Web proxy service**.
   The **Web Proxy Service** page displays.
3. Click the **Dynamic Single Sign-On Profiles** tab.

4. Click the + (New) icon.

   The **Dynamic Single Sign-On Profile** page displays.

5. Type a **Name** and **Description**.

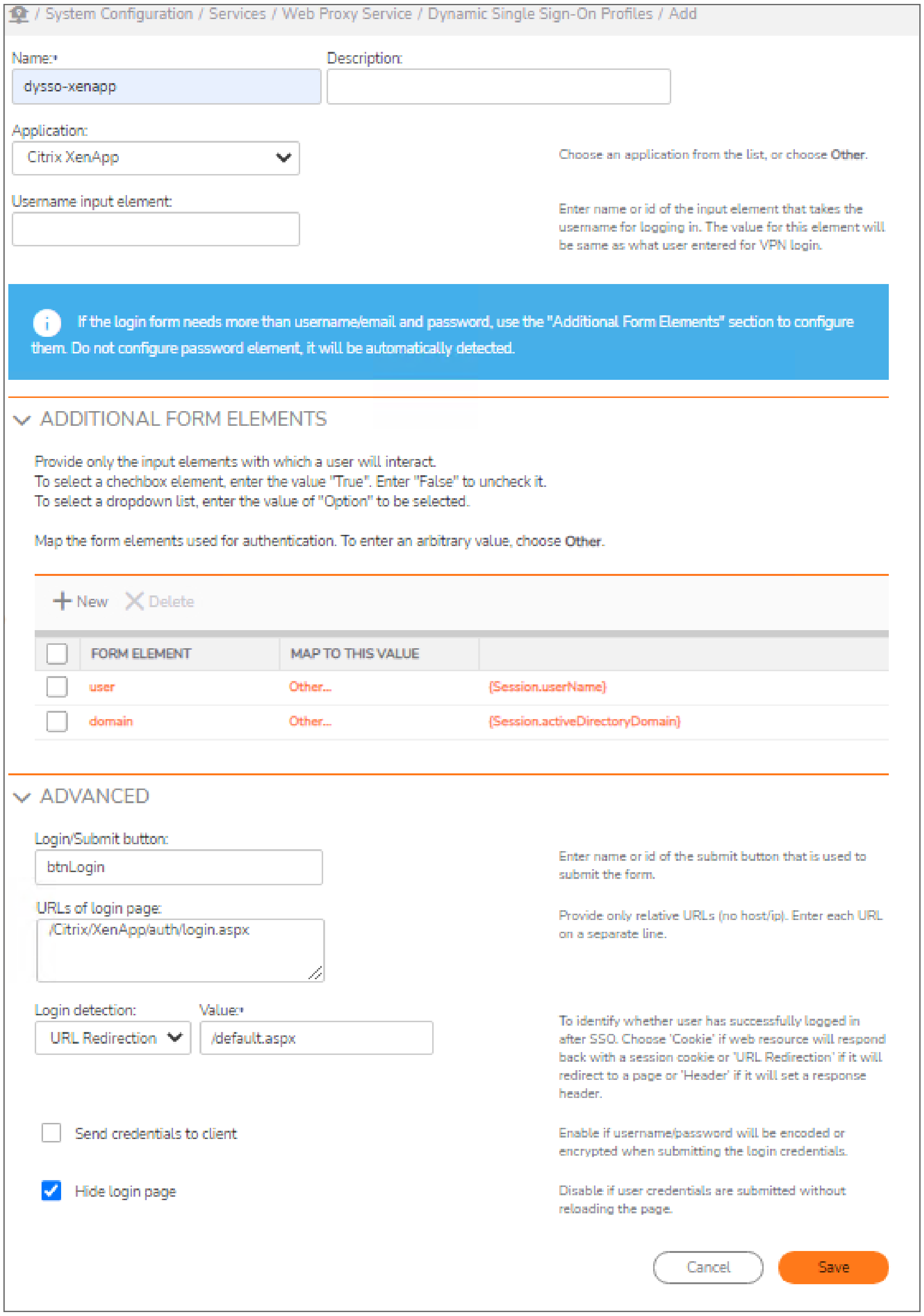
6. Select **Citrix XenApp** from the **Application** list.



Choose an application from the list, or choose Other.

Enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user entered for VPN login.

ⓘ **NOTE:** Selecting Citrix XenApp from the Application list loads the preconfigured system profile for citrix xenapp.



/ System Configuration / Services / Web Proxy Service / Dynamic Single Sign-On Profiles / Add

Name:* dysso-xenapp

Description:

Application: Citrix XenApp

Choose an application from the list, or choose **Other**.

Username input element:

Enter name or id of the input element that takes the username for logging in. The value for this element will be same as what user entered for VPN login.

If the login form needs more than username/email and password, use the "Additional Form Elements" section to configure them. Do not configure password element, it will be automatically detected.

ADDITIONAL FORM ELEMENTS

Provide only the input elements with which a user will interact.
To select a chechbox element, enter the value "True". Enter "False" to uncheck it.
To select a dropdown list, enter the value of "Option" to be selected.

Map the form elements used for authentication. To enter an arbitrary value, choose **Other**.

□	FORM ELEMENT	MAP TO THIS VALUE	
□	user	Other...	{Session.userName}
□	domain	Other...	{Session.activeDirectoryDomain}

ADVANCED

Login/Submit button: btnLogin

Enter name or id of the submit button that is used to submit the form.

URLs of login page: /Citrix/XenApp/auth/login.aspx

Provide only relative URLs (no host/ip). Enter each URL on a separate line.

Login detection: URL Redirection

Value:* /default.aspx

To identify whether user has successfully logged in after SSO. Choose 'Cookie' if web resource will respond back with a session cookie or 'URL Redirection' if it will redirect to a page or 'Header' if it will set a response header.

□ Send credentials to client

Enable if username/password will be encoded or encrypted when submitting the login credentials.

☑ Hide login page

Disable if user credentials are submitted without reloading the page.

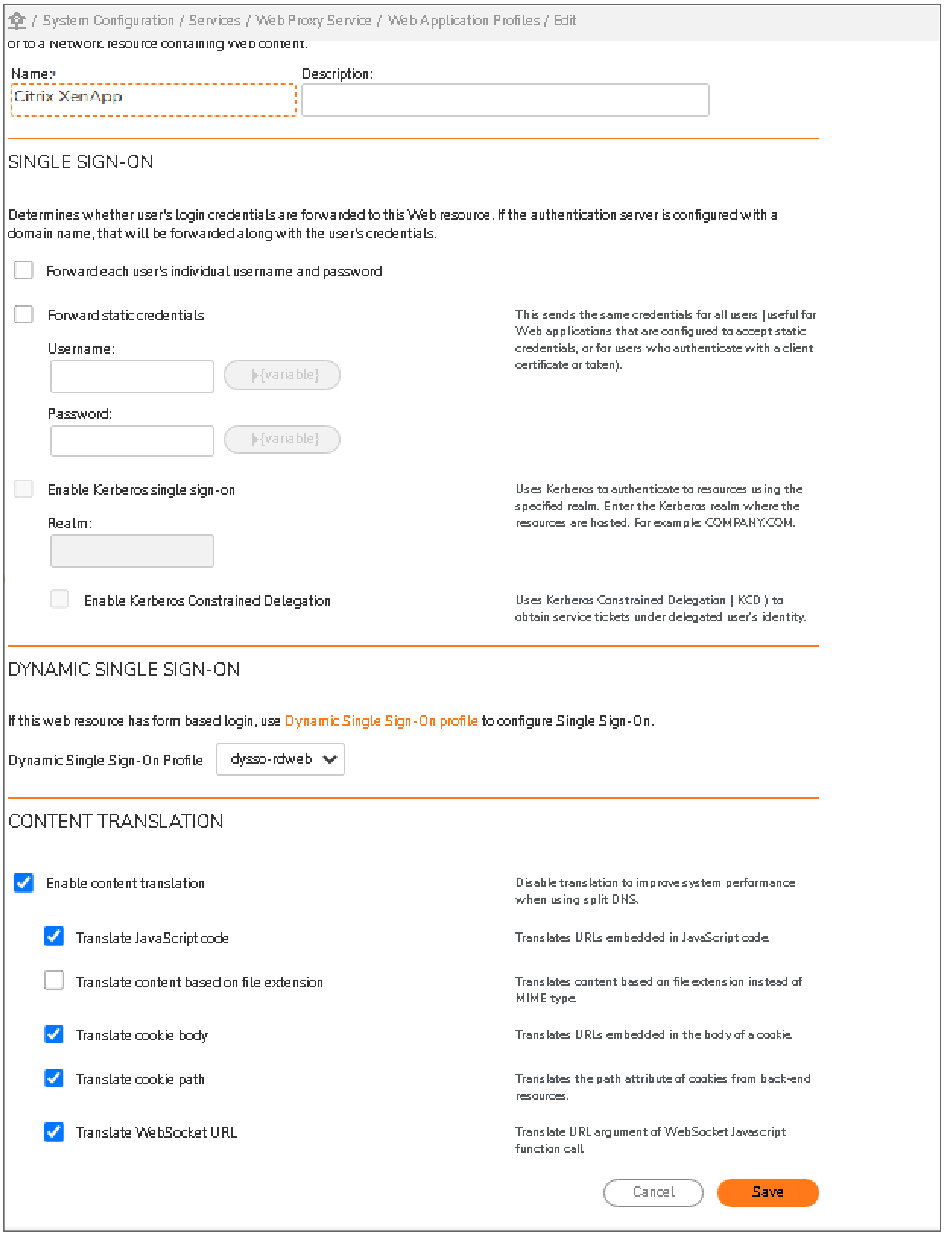
7. Click **Save**.

Creating Web Application Profile

1. In the AMC, navigate to **System Configuration** > **Services**.
2. In the **Access Services** section, click the **Configure** under **Web proxy service**.

The **Web Proxy Service** page displays.

3. Click the **Web Application Profiles** tab.
4. Click the + (New) icon.
   The **Add Web Application Profile** page displays.
5. Enter the name and description.
6. Configure **Dynamic Single Sign-On** by adding the above created Citrix XenApp Dynamic SSO profile.
7. Under **Content translation**, select the **Translate WebSocket URL** checkbox.



/ System Configuration / Services / Web Proxy Service / Web Application Profiles / Edit

or to a Network resource containing web content.

Name:* Citrix XenApp

Description:

SINGLE SIGN-ON

Determines whether user's login credentials are forwarded to this Web resource. If the authentication server is configured with a domain name, that will be forwarded along with the user's credentials.

□ Forward each user's individual username and password

□ Forward static credentials — This sends the same credentials for all users (useful for Web applications that are configured to accept static credentials, or for users who authenticate with a client certificate or token).

Username:

Password:

□ Enable Kerberos single sign-on — Uses Kerberos to authenticate to resources using the specified realm. Enter the Kerberos realm where the resources are hosted. For example COMPANY.COM.

Realm:

□ Enable Kerberos Constrained Delegation — Uses Kerberos Constrained Delegation (KCD) to obtain service tickets under delegated user's identity.

DYNAMIC SINGLE SIGN-ON

If this web resource has form based login, use Dynamic Single Sign-On profile to configure Single Sign-On.

Dynamic Single Sign-On Profile: dysso-rdweb

CONTENT TRANSLATION

☑ Enable content translation — Disable translation to improve system performance when using split DNS.

☑ Translate JavaScript code — Translates URLs embedded in JavaScript code.

□ Translate content based on file extension — Translates content based on file extension instead of MIME type.

☑ Translate cookie body — Translates URLs embedded in the body of a cookie.

☑ Translate cookie path — Translates the path attribute of cookies from back-end resources.

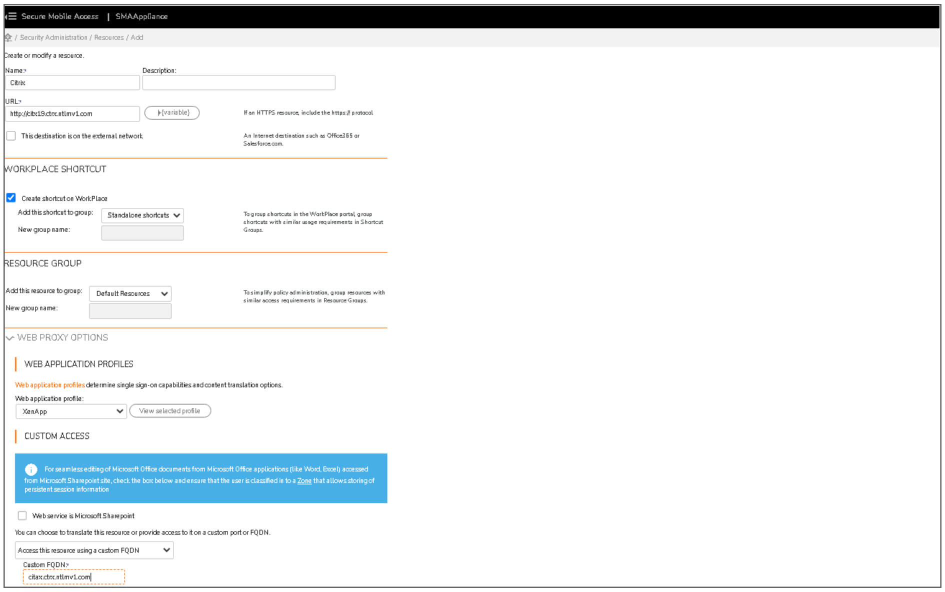
☑ Translate WebSocket URL — Translate URL argument of WebSocket Javascript function call

8. Click **Save**.

Creating Citrix XenApp URL resource with custom access

1. In the AMC, navigate to **Security Administration** > **Resources**.
2. Click the + (New) icon.
3. Select URL from the drop-down list.

   The **Add Resource - URL** page displays.
4. In the **Name** field, enter the name for this URL resource.
5. In the **URL** field, enter the URL.
6. Select the **Create Shortcut on WorkPlace** check box.
7. Expand **Web Proxy Options** and do the following:
   a. Under **Web Application profile**, select the created web application profile.
   b. Under **Custom Access** section, select **Access this resource using a custom FQDN**.
   c. Provide **Custom FQDN**.


Secure Mobile Access | SMAAppliance
/ Security Administration / Resources / Add
{variable}
View selected profile

Create or modify a resource.

Name: Citrix

Description:

URL: http://citx19.ctrx.ntlmv1.com

If an HTTPS resource, include the https:// protocol

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUT

☑ Create shortcut on WorkPlace

Add this shortcut to group: Standalone shortcuts

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

RESOURCE GROUP

Add this resource to group: Default Resources

New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

WEB PROXY OPTIONS

WEB APPLICATION PROFILES

Web application profiles determine single sign-on capabilities and content translation options.

Web application profile: XenApp

CUSTOM ACCESS

For seamless editing of Microsoft Office documents from Microsoft Office applications (like Word, Excel) accessed from Microsoft Sharepoint site, check the box below and ensure that the user is classified in to a Zone that allows storing of persistent session information

□ Web service is Microsoft Sharepoint

You can choose to translate this resource or provide access to it on a custom port or FQDN.

Access this resource using a custom FQDN

Custom FQDN: citax.ctrx.ntlmv1.com

8. Click **Save**.

Adding Citrix Xenapp in start page

1. In the AMC, navigate to User Access > Workplace.
2. Click the Shortcuts tab.
3. Select **Citrix XenApp**.
4. Click **Next** to display the **Advanced** page.

5. Select the **All devices** check box.
6. In the **Start page** field, enter URL `/Citrix/XenApp/auth/login.aspx`.
7. Click **Save**.

Kerberos Constrained Delegation

SMA supports Kerberos Constrained Delegation (KCD). Kerberos Constrained Delegation (KCD) provides authentication support using an existing Kerberos infrastructure, which does not need to trust front-end services to delegate a service.

With Kerberos Constrained Delegation (KCD), users who are authenticated using non-Kerberos methods, such as Certificate, Smart Card, or RADIUS, can gain access to Kerberos protected resources without having to enter any additional credentials. For example, a user that authenticates using Single Sign-On (SSO), rather than Kerberos, is allowed access to Kerberos protected web resources.

Most Single Sign-On (SSO) methods rely on the conventional username/password credentials. However, these credentials do not work with Certificate, Smart Card, or RADIUS authentication. With Kerberos Constrained Delegation (KCD), the administrator configures the usernames and passwords for Kerberos Constraine Delegation (KCD).

Microsoft’s Kerberos v5 extension is called Services for Users (S4U) and is compromised of two parts:

- S4U2Self
- S4U2Proxy

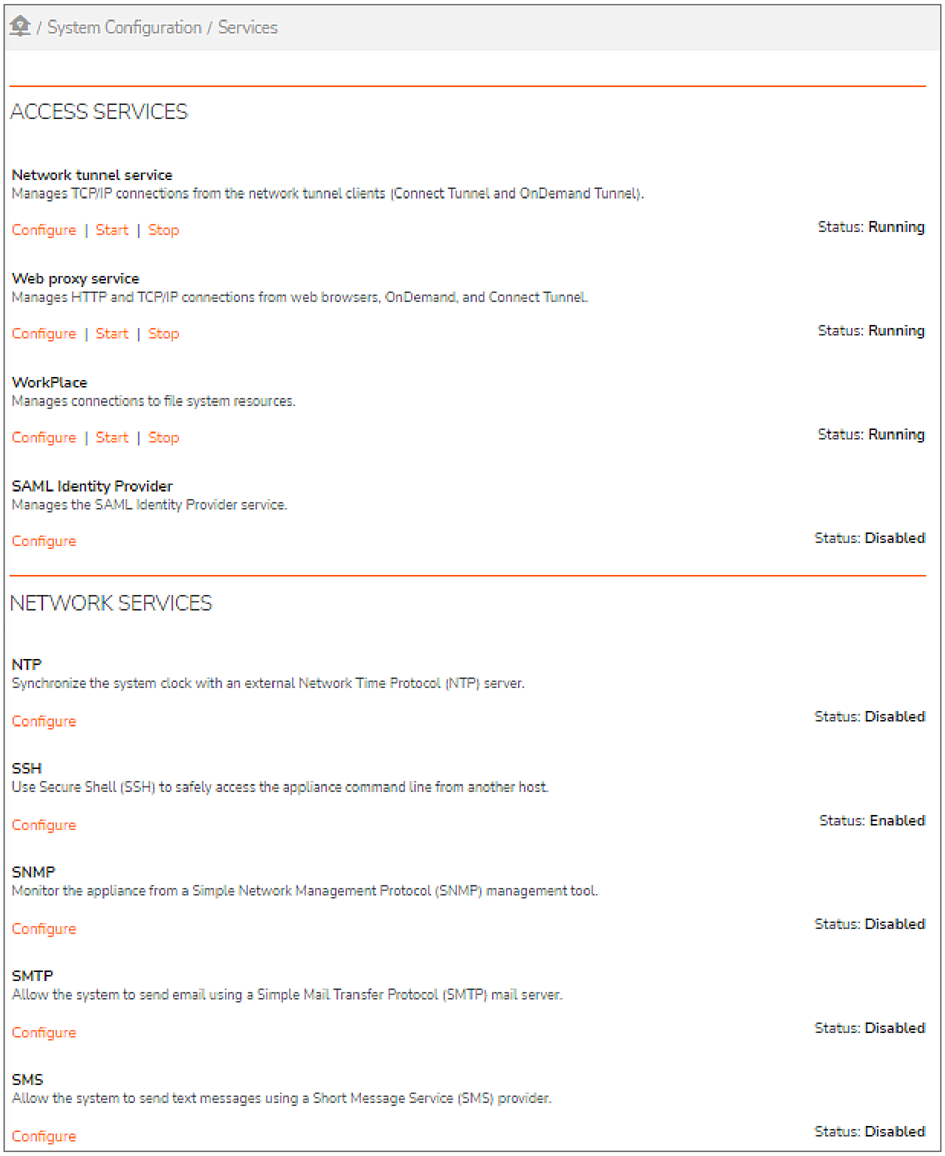
S4U2Self allows a service to obtain a service ticket to itself on behalf of a client and is usually used with a client certificate. S4U2Self is the Kerberos Protocol Transition extension.

S4U2Proxy allows a service to obtain a service ticket to an arbitrary service on behalf of a user with only the user's service ticket. The services are constrained by the administrator. S4U2Proxy is the Kerberos Constrained Delegation (KCD) extension.

Configuring Kerberos Constrained Delegation

To enable Kerberos Constrained Delegation (KCD):

1. Navigate to **System Configuration > Services**.



/ System Configuration / Services

ACCESS SERVICES

Network tunnel service
Manages TCP/IP connections from the network tunnel clients (Connect Tunnel and OnDemand Tunnel).
Configure | Start | Stop — Status: Running

Web proxy service
Manages HTTP and TCP/IP connections from web browsers, OnDemand, and Connect Tunnel.
Configure | Start | Stop — Status: Running

WorkPlace
Manages connections to file system resources.
Configure | Start | Stop — Status: Running

SAML Identity Provider
Manages the SAML Identity Provider service.
Configure — Status: Disabled

NETWORK SERVICES

NTP
Synchronize the system clock with an external Network Time Protocol (NTP) server.
Configure — Status: Disabled

SSH
Use Secure Shell (SSH) to safely access the appliance command line from another host.
Configure — Status: Enabled

SNMP
Monitor the appliance from a Simple Network Management Protocol (SNMP) management tool.
Configure — Status: Disabled

SMTP
Allow the system to send email using a Simple Mail Transfer Protocol (SMTP) mail server.
Configure — Status: Disabled

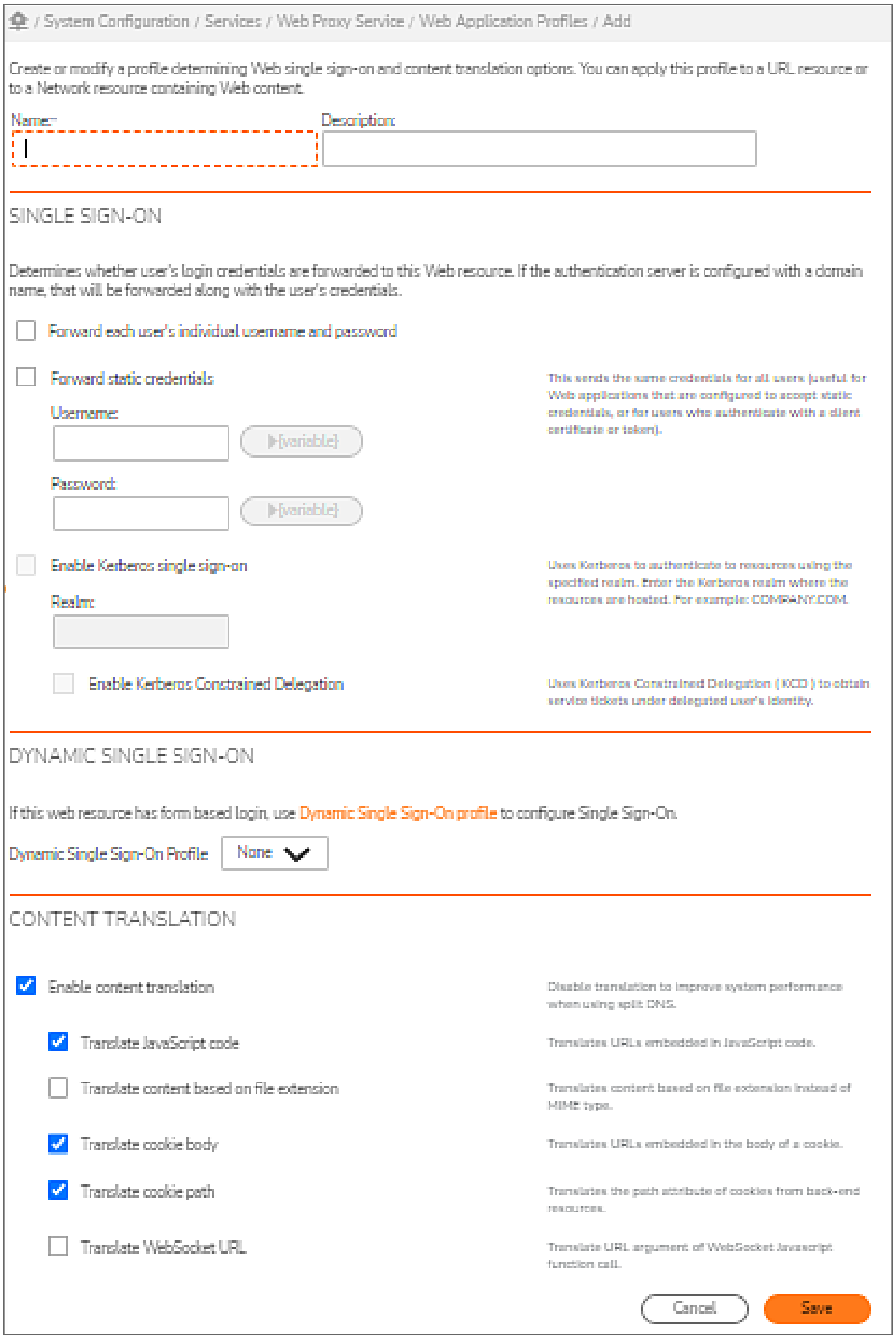
SMS
Allow the system to send text messages using a Short Message Service (SMS) provider.
Configure — Status: Disabled

2. Under **Web proxy service**, click **Configure.**

   The **Web Proxy Service** page displays.

3. Click the **Web Application Profiles** tab.
4. From the list of **Web Proxy Services**, select the web proxy service you want.

   The **Edit Web Application Profile** page displays.



/ System Configuration / Services / Web Proxy Service / Web Application Profiles / Add

Create or modify a profile determining Web single sign-on and content translation options. You can apply this profile to a URL resource or to a Network resource containing Web content.

Name:*

Description:

SINGLE SIGN-ON

Determines whether user's login credentials are forwarded to this Web resource. If the authentication server is configured with a domain name, that will be forwarded along with the user's credentials.

☐ Forward each user's individual username and password

☐ Forward static credentials — This sends the same credentials for all users (useful for Web applications that are configured to accept static credentials, or for users who authenticate with a client certificate or token).

Username:

Password:

☐ Enable Kerberos single sign-on — Uses Kerberos to authenticate to resources using the specified realm. Enter the Kerberos realm where the resources are hosted. For example: COMPANY.COM.

Realm:

☐ Enable Kerberos Constrained Delegation — Uses Kerberos Constrained Delegation (KCD) to obtain service tickets under delegated user's identity.

DYNAMIC SINGLE SIGN-ON

If this web resource has form based login, use Dynamic Single Sign-On profile to configure Single Sign-On.

Dynamic Single Sign-On Profile: None

CONTENT TRANSLATION

☑ Enable content translation — Disable translation to improve system performance when using split DNS.

☑ Translate JavaScript code — Translates URLs embedded in JavaScript code.

☐ Translate content based on file extension — Translates content based on file extension instead of MIME type.

☑ Translate cookie body — Translates URLs embedded in the body of a cookie.

☑ Translate cookie path — Translates the path attribute of cookies from back-end resources.

☐ Translate WebSocket URL — Translate URL argument of WebSocket Javascript function call.

5. Select the check boxes for the options you want:

   - **Enable Kerberos Constrained Delegation** – The **Enable Kerberos Constrained Delegation** option should be checked only if the **Kerberos Single Sign-On** option is checked.

- **Enable fallback** – The **Enable fallback** option should be checked only if the **Enable Kerberos Constrained Delegation** option is checked.

  The **Enable fallback** option prompts the user to enter their credentials again if KCD has failed for some reason. If **Enable fallback** is unchecked and KCD has failed, an error page is displayed.

  > ⓘ **NOTE:** On Firefox, **Enable fallback** works only if both Negotiate and NTLM are enabled on the backend resource, in their respective order. **Enable fallback** does not work on Safari in this case. Safari displays a prompt to re-enter credentials, but it keeps failing. **Enable fallback** works only when **NTLM** is the only authentication provider on the backend, which is not a supported configuration for KCD.

6. If the selected web resource has form based login, use Dynamic Single Sign-On profile to configure Single Sign-On. For more information, see Creating Forms-Based Dynamic Single Sign-On Profiles.
7. Click **Save**.

Configuring SMA Support for Microsoft Outlook Anywhere

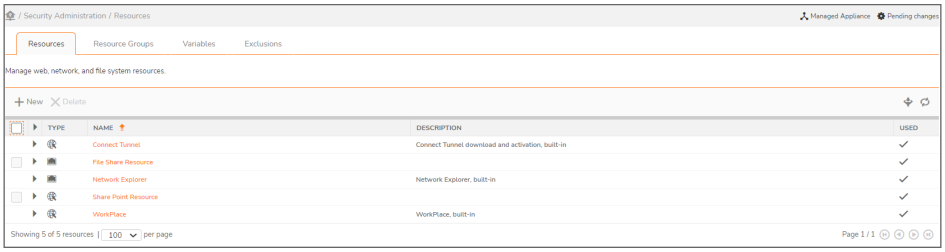
SMA supports Microsoft Outlook Anywhere for Windows Outlook Clients. Outlook Anywhere is basically an Outlook client that connects to the Microsoft Exchange server using one of these protocols:

- Remote Procedure Call (RPC) over HTTP
- MAPI over HTTP

Microsoft Outlook Anywhere allows end users with Microsoft Office Outlook to connect to their Exchange servers over the Internet from outside the corporate network.

To configure SMA Support for Outlook Anywhere:

1. In the AMC, navigate to **Security Administration > Resources**.



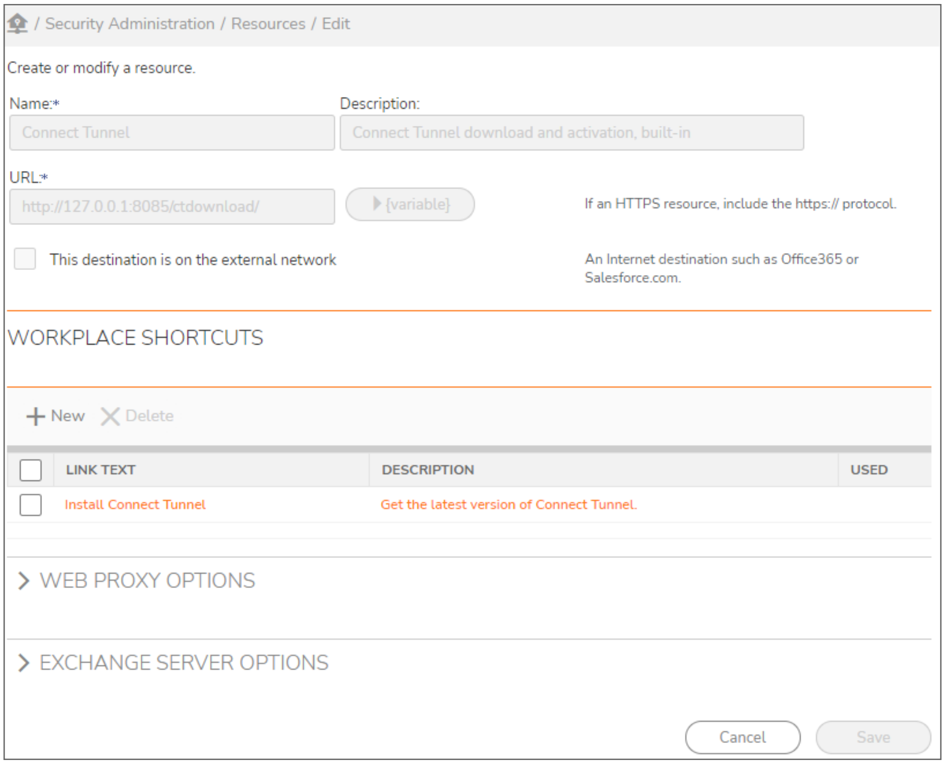
Manage web, network, and file system resources.

TYPE	NAME	DESCRIPTION	USED
	Connect Tunnel	Connect Tunnel download and activation, built-in	✓
	File Share Resource		✓
	Network Explorer	Network Explorer, built-in	✓
	Share Point Resource		✓
	WorkPlace	WorkPlace, built-in	✓

Showing 5 of 5 resources | 100 per page

Page 1 / 1

2. Click on the resource you want to edit. The **Edit Resource** page displays.



/ Security Administration / Resources / Edit

Create or modify a resource.

Name:* Connect Tunnel

Description: Connect Tunnel download and activation, built-in

URL:* http://127.0.0.1:8085/ctdownload/

If an HTTPS resource, include the https:// protocol.

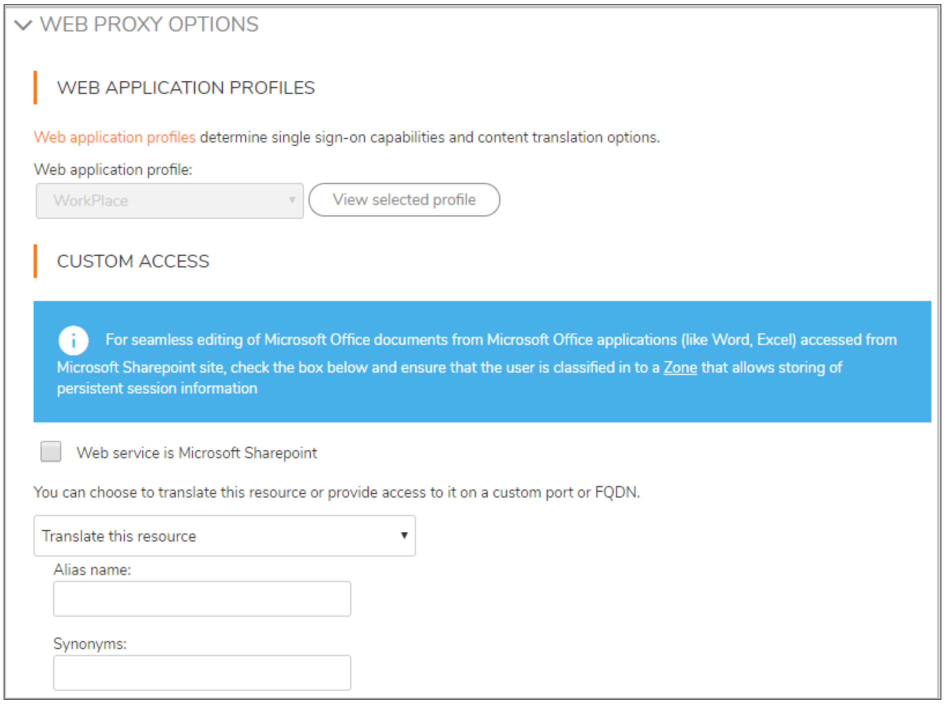
□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUTS

□	LINK TEXT	DESCRIPTION	USED
□	Install Connect Tunnel	Get the latest version of Connect Tunnel.	

3. Click on **Web Proxy Options** panel to expand it.



WEB PROXY OPTIONS

WEB APPLICATION PROFILES

Web application profiles determine single sign-on capabilities and content translation options.

Web application profile: WorkPlace

CUSTOM ACCESS

For seamless editing of Microsoft Office documents from Microsoft Office applications (like Word, Excel) accessed from Microsoft Sharepoint site, check the box below and ensure that the user is classified in to a Zone that allows storing of persistent session information

□ Web service is Microsoft Sharepoint

You can choose to translate this resource or provide access to it on a custom port or FQDN.

Translate this resource

Alias name:

Synonyms:

4. In **Web application profile** drop-down menu, select **OWA/Single Sign-on**.

5. Click on the **Exchange Server options** panel to open it.
6. Select the check box for **Enable Exchange ActiveSync and Outlook Anywhere access to this resource**.
7. In the **Exchange server FQDN** field, enter the external FQDN URL of the user's Exchange server.

   This should be the same value that is configured as the external FQDN URL for Outlook Anywhere services (RPC/HTTP and MAPI/HTTP protocols and EWS service) at the Exchange server.
8. In the **Realm** drop-down menu, select the **Realm** that you want.
9. In the **Exchange Autodiscover FQDN**, enter the FQDN of the Exchange Autodiscover service, for example: **autodiscover.example.com**.

   The Autodiscover FQDN is used by the Outlook client to determine the Autodiscover service which enables Outlook to configure the Outlook options by just accepting the user's Email address. For example, the email address, `user@yourcompany.com`, would have an Autodiscover FQDN of `autodiscover.yourcompany.com`.

   The name autodiscover.yourcompany.com must be configured in a public DNS server with the public IP address of the appliance.
10. Leave the **Fallback Exchange server URL** field blank for Outlook Anywhere.

    ⓘ **NOTE:** For Outlook Anywhere using RPC over HTTP, only basic authentication is supported. So, the backend exchange server should be configured to support basic authentication for Outlook Anywhere - ExternalClientAuthenticationMethod. For MAPI over HTTP, any authentication method can be configured.

    ⓘ **NOTE:** For requests coming from the Outlook client, zone classification is done without any attributes, and the user is classified into whichever zone it matches.

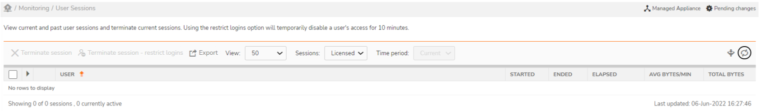
    The Autodiscover FDQN is also displayed on the **System Configuration > Network Settings** page.

Viewing User Sessions

SMA users that are using Exchange ActiveSync and Outlook Anywhere can be displayed on the **Monitoring > User > Sessions** page by selecting **Exchange** as the filter from the **Agents** drop-down menu. The **Exchange** filter will filter Exchange ActiveSync and Outlook Anywhere users. The detailed view will show what the Access Agent is for that user.

To view Outlook Anywhere user sessions:

1. In the AMC, navigate to **Monitoring > User Sessions** page.



View current and past user sessions and terminate current sessions. Using the restrict logins option will temporarily disable a user's access for 10 minutes.

□	USER	STARTED	ENDED	ELAPSED	AVG BYTES/MIN	TOTAL BYTES

No rows to display

Showing 0 of 0 sessions , 0 currently active

Last updated: 06-Jun-2022 16:27:46

2. Click the **Filter** icon on the right to display the available filters.
3. In the **Agent** drop-down menu, select **Exchange**.

   If you hover over the **Exchange Server** option, it shows that **Exchange ActiveSync and Outlook Anywhere** users will be displayed for this option.

4. Click **Refresh** to see the new list of users.
5. To see a detailed view of any user listed, click on that user.

   The **Access Agent** field in the detailed view shows which agent the user is using. Outlook Anywhere will be shown in the **Access-Agent** field.

Access Control Rules

Access control rules determine which resources are available to users or groups. Rules can be defined broadly to provide access using any method, or defined narrowly so that only a specific access method—Web browser, Connect and OnDemand, or Network Explorer—is permitted.

In addition to evaluating whether users can access resources based on who they are, access control rules can also factor in the trustworthiness of users' access points using End Point Control zones and device profiles, which are described in Managing EPC with Zones and Device Profiles.

Topics:

- Configuring Access Control Rules
- Resolving Deny Rule Incompatibilities
- Resolving Invalid Destination Resources

Configuring Access Control Rules

As your network changes over time, you will need to configure the access control rules that determine what application resources are available to your various users and groups.

Before adding an access control rule, carefully examine your existing rules; you might find that you can modify a rule instead of creating a new one. You can also copy an existing rule and then modify its parameters.

If you add a new rule, review your current configuration to determine where the new rule should fit in the rule order. New rules are added to the top of the list by default; you can then move them to their proper positions.

Topics:

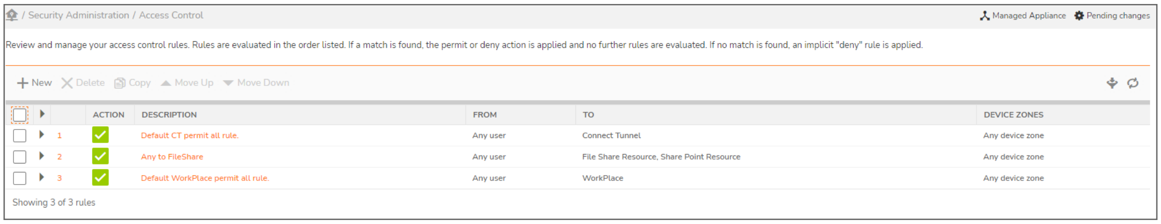
- Viewing Access Control Rules
- Access Control Rules for Bi-Directional Connections
- Requirements for Reverse and Cross-Connections
- Securing Application Ports for Reverse Connections
- Adding Access Control Rules for a Forward Connection
- Specifying Advanced Access Control Rule Attributes
- Adding Access Control Rules for a Reverse Connection
- Adding a Pair of Access Control Rules for a Cross-Connection
- Configuring Advanced Access Control Rule Attributes
- Access Methods and Advanced Options
- Adding Users and Resources From Within Access Control Rules
- Editing, Copying, and Deleting Access Control Rules

Viewing Access Control Rules

Access control rules are displayed in numerical order on the **Access Control** page. The appliance evaluates the rules in numbered order. All access control rules are displayed by default, but you can use the **Filters** settings to filter them by resource type or other criteria.

To view access control rules:

1. In AMC, navigate to **Security Administration > Access Control**.



/ Security Administration / Access Control

Review and manage your access control rules. Rules are evaluated in the order listed. If a match is found, the permit or deny action is applied and no further rules are evaluated. If no match is found, an implicit "deny" rule is applied.

			ACTION	DESCRIPTION	FROM	TO	DEVICE ZONES
□		1	✓	Default CT permit all rule.	Any user	Connect Tunnel	Any device zone
□		2	✓	Any to FileShare	Any user	File Share Resource, Share Point Resource	Any device zone
□		3	✓	Default WorkPlace permit all rule.	Any user	WorkPlace	Any device zone

Showing 3 of 3 rules

2. By default, all rules that you have created, regardless of resource type, are displayed. Use the **Filters** section to display a subset of rules. For information about using filters, see Filters. To see a particular rule set, select one of the following from the **Method** drop-down menus in **Filters**; see the below table.

Rule Set Descriptions

Method	Description
Web browser	Display rules controlling access to Web-based (HTTP and HTTPS) resources.
Connect Tunnel/OnDemand Mapped Mode	Display rules controlling access to client/server (TCP/IP) resources

Network Explorer	Display rules controlling access to Windows file system resources using WorkPlace.

3. Review the data shown in the access control rule list:

   - Use the check box column to select one or more rules to delete, copy, or reorder (using the **Move Up** and **Move Down** buttons).
   - The number column indicates the order in which the rule will be evaluated. To edit a rule, click its corresponding number.
   - To display configuration details and the objects referenced in a rule, click the plus sign (**+**) next to it.
   - The **Action** column indicates whether a rule permits or denies access, or is ignored; see the below table.

   Rule Action Indicators

Indicator	Description
Green	Access is permitted.
Red	Access is denied.
Gray	The rule is not evaluated. (Disabling a rule is a convenient way to temporarily stop using a rule without deleting it).

   - The **Description** column lists the descriptive text you typed when creating the rule.
   - The **From** column indicates the users to whom the rule applies (**Any**: all users). In the case of a reverse connection, this column indicates the resource that is connecting to a user or group. See Access Control Rules for Bi-Directional Connections.
   - The **To** column lists the destination resources to which the rule applies (**Any**: all users). In the case of a reverse connection, this column can also indicate the user or group that is connecting back to a resource. See Access Control Rules for Bi-Directional Connections.
   - The **Method** column indicates whether a specific access method is associated with a rule. A globe icon signifies Web browser-based HTTP access; a globe icon with a folder represents Network Explorer, which provides Web access to file system resources; the Secure Mobile Access logo indicates access using the Connect Tunnel or proxy clients, or the OnDemand Tunnel or proxy agents. **Any** indicates that the rule applies to all access methods.
   - The **Zone** column indicates whether an access rule is associated with a particular End Point Control zone. EPC zones are used to classify a connection request based on the attributes of the client device. *Any* indicates the rule applies to all EPC zones; a red **Restricted** icon indicates that the rule controls access for one or more specific zones.

Access Control Rules for Bi-Directional Connections

VPN connections typically involve forward connections, which are initiated by a user to a client/server resource. However, if you deploy SonicWall’s network tunnel clients (Connect Tunnel or OnDemand Tunnel) to your users, bi-directional connections are enabled.

With the SonicWall VPN, bi-directional connections encompass:

- Forward connections from a VPN user to a client/server resource. See Adding Access Control Rules for a Forward Connection.
- Reverse connections from a client/server resource to a VPN user. An example of a reverse connection is an SMS server that "pushes" a software update to a user's machine. See Adding Access Control Rules for a Reverse Connection.
- Cross-connections refer specifically to VoIP (Voice over Internet Protocol) applications that enable one VPN user to telephone another VPN user. Cross-connections require a pair of access control rules: one for the forward connection and one for the reverse connection. See Adding a Pair of Access Control Rules for a Cross-Connection.

Other examples of bi-directional connections include an FTP server that downloads files to or uploads files from a VPN user, and remote Help Desk applications.

Requirements for Reverse and Cross-Connections

Before you can configure access control rules for reverse connections and cross-connections, these requirements must be met:

- The network tunnel service must be running on the appliance. On the **Services** page in AMC, check the status for **Network tunnel service**; it should be **Running**.
- An IP address pool for the network tunnel clients must be configured. See Configuring IP Address Pools for information on how to set one up.
- Users who have access to a VoIP application must belong to a community that is configured to deploy the network tunnel clients (Connect Tunnel or OnDemand Tunnel) to their computers. See Creating and Configuring Communities.

Securing Application Ports for Reverse Connections

By default, reverse connections from resources to users have access to all ports on users' computers. For enhanced security, create access control rules for reverse connections that confine access to the ports that an application specifically uses. Consult the application's documentation for information about which firewall ports must be open in order to use the application.

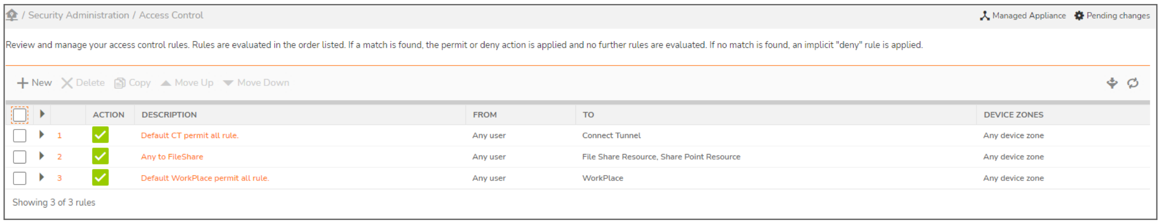
When configuring an access rule for a reverse connection, use the **Destination restrictions** option to confine access to the ports required by the application making the reverse connection. See Configuring Advanced Access Control Rule Attributes for information on this option.

Adding Access Control Rules for a Forward Connection

Perform the following steps to add an access control rule for a forward connection from users to destination resources. For information about creating an access control rule for a cross-connection (for example, for a VoIP application), see Adding a Pair of Access Control Rules for a Cross-Connection.

To add an access control rule for a forward connection:

1. In AMC, navigate to **Security Administration > Access Control**.



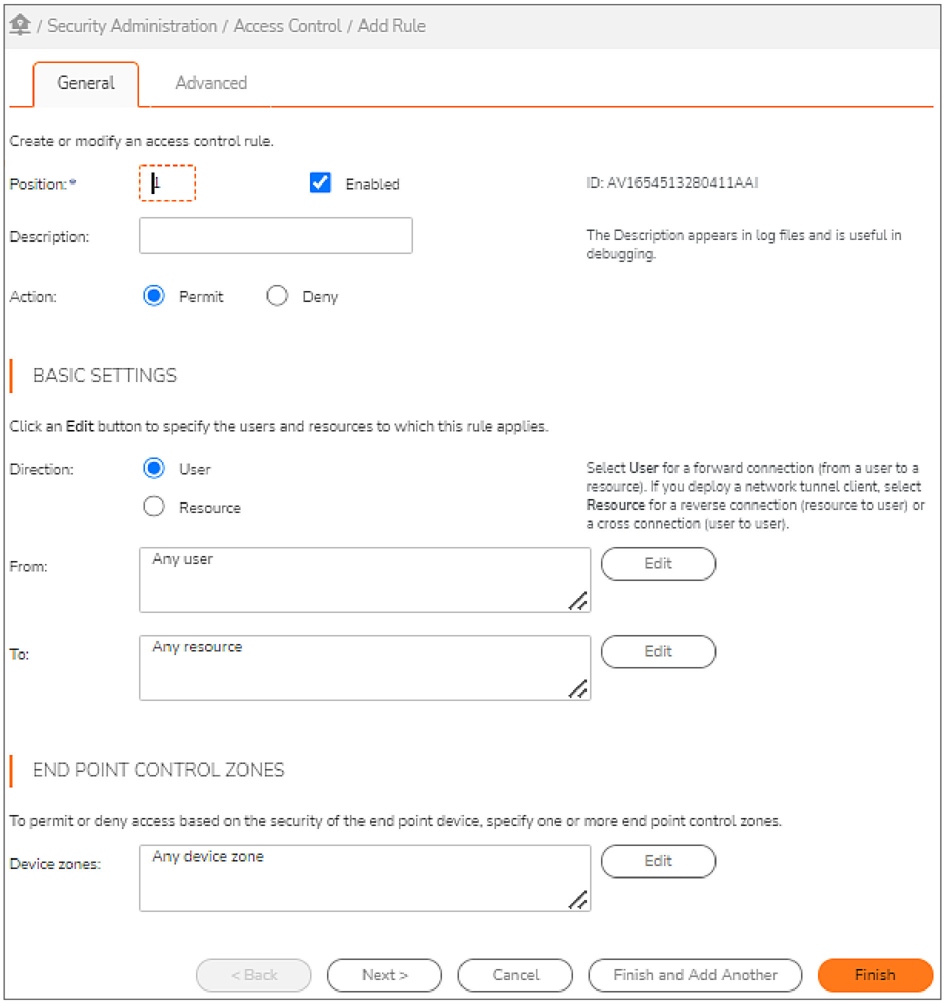
Review and manage your access control rules. Rules are evaluated in the order listed. If a match is found, the permit or deny action is applied and no further rules are evaluated. If no match is found, an implicit "deny" rule is applied.

□		ACTION	DESCRIPTION	FROM	TO	DEVICE ZONES
□	1	✓	Default CT permit all rule.	Any user	Connect Tunnel	Any device zone
□	2	✓	Any to FileShare	Any user	File Share Resource, Share Point Resource	Any device zone
□	3	✓	Default WorkPlace permit all rule.	Any user	WorkPlace	Any device zone

Showing 3 of 3 rules

2. Click the **+** (New) icon.

   The **Add Access Rule** page displays.



Create or modify an access control rule.

Position: * 1 ☑ Enabled ID: AV1654513280411AAI

Description:

The Description appears in log files and is useful in debugging.

Action: ● Permit ○ Deny

BASIC SETTINGS

Click an **Edit** button to specify the users and resources to which this rule applies.

Direction: ● User ○ Resource

Select **User** for a forward connection (from a user to a resource). If you deploy a network tunnel client, select **Resource** for a reverse connection (resource to user) or a cross connection (user to user).

From: Any user

To: Any resource

END POINT CONTROL ZONES

To permit or deny access based on the security of the end point device, specify one or more end point control zones.

Device zones: Any device zone

3. Type a number in the **Number** field to specify the rule's position in the access rule list. By default, new rules are added to the top of the list, but you can use this box to place the rule anywhere you want. For example, if you assign the number 3 to a new rule, the new rule will be inserted before the current rule **3**

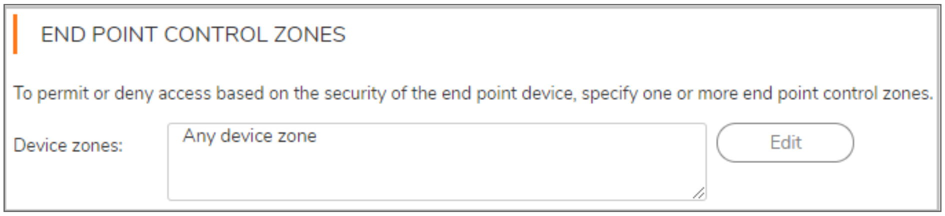
(which will become rule **4**). This field is required.

To the right of the **Number** field is a unique identifier for the rule, which you can use for troubleshooting. When you add or change a rule, for example, the Management Console audit log shows a record of the change using this ID. Logging is described in detail in System Logging and Monitoring.

4. In the **Description** field, type a descriptive comment about the rule. This step is optional, but a description can be helpful when viewing your list of rules later; it also appears in log files where can be useful for debugging. The **ID** is a unique identifier automatically assigned by AMC; it cannot be edited.
5. Use the **Action** buttons to specify whether the rule will be used to **Permit** or **Deny** access, or if the rule is **Disabled**.
6. Complete the information listed under **Basic settings**:
   - Click **User** to configure a forward connection (from a user to a resource).
   - If you deploy a network tunnel client, click **Resource** to create a rule controlling a reverse connection (resource to user) or a cross-connection (user to user). The network tunnel service must be configured with an IP address pool before you can use reverse connections (see Configuring IP Address Pools).
   - The **From** field specifies the users or user groups to whom the rule applies. Click **Edit** to select from a list of users and groups. If no users or groups are specified, the value for this field is **Any** *user*.
   - The **To** field specifies the destination resources or resource groups for the rule. Click **Edit** to select from a list of resources. If no destination resources are selected, the value for this field is **Any** *resource*. A warning appears if the destination resource contains a wildcard indicating a Mobile Connect incompatibility.

ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

7. In the **End Point Control zones** area, select the zones from which you will permit or deny access to the resources. Click **Edit** to select from a list. The default for this field is **Any** zone. See Managing EPC with Zones and Device Profiles for information about configuring and using zones.


END POINT CONTROL ZONES

To permit or deny access based on the security of the end point device, specify one or more end point control zones.

Device zones: Any device zone

8. Click **Next** to configure additional settings (see Specifying Advanced Access Control Rule Attributes), or click **Finish** to save the current settings.

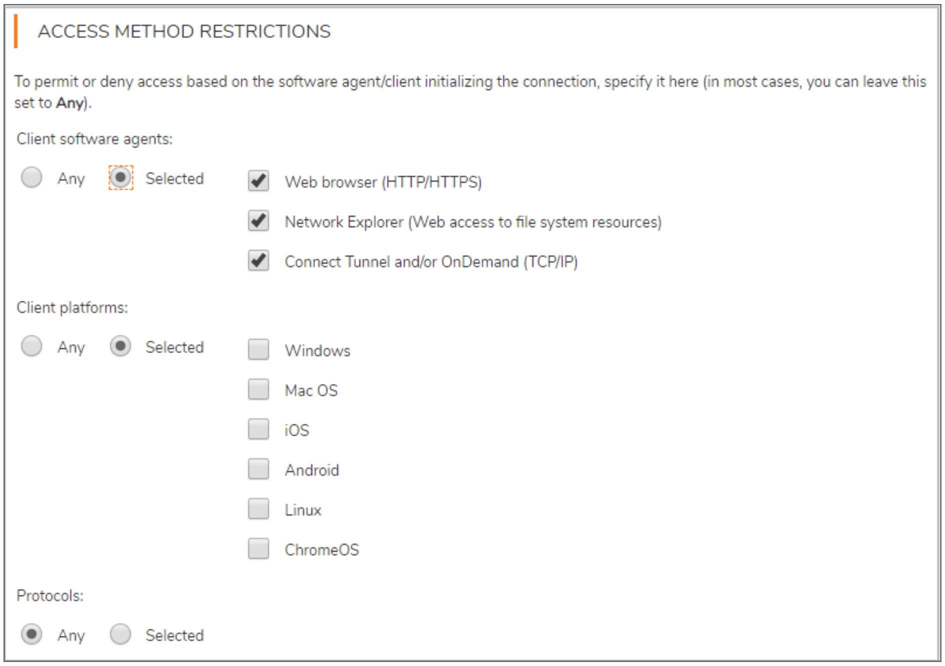
Specifying Advanced Access Control Rule Attributes

For most rules, a basic configuration that includes users or groups, destination resources, and access methods is sufficient. However, additional options are available to provide even tighter access. For example, you can control a connection based on the location of the user (by IP address). Source networks are referenced in an access rule to permit or deny a connection to a destination resource based on the location from which the request originates, provides even greater security.

To configure advanced settings for an access control rule:

1. In AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon.

   The **Add Access Rule** page displays.
3. Click **Next** to display the **Advanced** tab.
4. In the **Access Method Restrictions** area, select one or more methods for access to the resource. **Any** is the recommended setting in most circumstances, unless your security environment requires you to use a particular method for access to a resource.



ACCESS METHOD RESTRICTIONS

To permit or deny access based on the software agent/client initializing the connection, specify it here (in most cases, you can leave this set to **Any**).

Client software agents:

○ Any ● Selected

☑ Web browser (HTTP/HTTPS)
☑ Network Explorer (Web access to file system resources)
☑ Connect Tunnel and/or OnDemand (TCP/IP)

Client platforms:

○ Any ● Selected

□ Windows
□ Mac OS
□ iOS
□ Android
□ Linux
□ ChromeOS

Protocols:

● Any ○ Selected

   a. When you select access methods, the advanced options are enabled or disabled based on whether they apply to the methods you specified. Click **Selected** to choose the access methods this rule will require; see the below table.

Client Software Agents

Access method	Description
Web browser (HTTP/HTTPS)	Manages access from HTTP or HTTPS resources for users connecting using a Web browser. The available **Advanced** settings are: • User's network address • Time and date restrictions

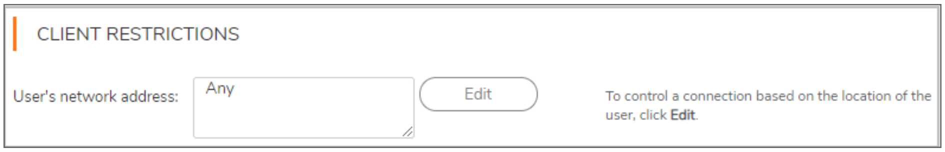
Network Explorer	Manages access from Windows file system resources for WorkPlace users connecting using Network Explorer. The available **Advanced** settings are: • User’s network address • Read/write permissions • Time and date restrictions
Connect Tunnel and/or OnDemand (TCP/IP)	Manages access from TCP/IP resources such as client/server applications, file servers, or databases, for users connecting with one of the following: • The Connect Tunnel or proxy clients • The OnDemand Tunnel or proxy agents For example, suppose you want to provide access to a network domain for users who have Connect or OnDemand, but you don’t want to allow browser access to Web resources within that domain. You can do that by creating a rule that specifies **Connect Tunnel and/or OnDemand Mapped Mode** as the only access method, and specifies the network domain in the **Client restrictions** area. The available **Advanced** settings are: • Protocols • User’s network address • Destination restrictions (ports) • Time and date restrictions

b. Click **Selected** to specify the **Protocols** (see the below table) that the network tunnel or proxy service will accept from the client. A brief description of each command is included here, but for more details, see http://www.ietf.org/rfc/rfc1928.txt.

Protocol Selecting

Protocol	Description
TCP	Enables normal TCP connections (for example, SSH, telnet, SCP, and so forth).
UDP	Allows the network tunnel or proxy service to make a UDP data transfer. This is necessary for operations such as streaming audio and Microsoft Outlook new-mail notification.
ICMP	(Internet Control Message protocol) Enables the ping and traceroute network troubleshooting commands. Selecting this option will configure the network tunnel or proxy service to allow these operations on your behalf. This option also enables ICMP packets to flow through the network tunnel or proxy service.

5. Under **Client restrictions**, in the **User's network address** field, specify the names of any source networks you want evaluated in the rule.



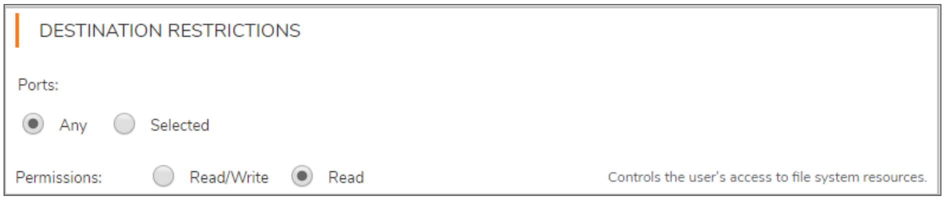
CLIENT RESTRICTIONS

User's network address: Any

To control a connection based on the location of the user, click **Edit**.

This is useful for controlling access based on the origin of the connection request. Click **Edit** to select from the list of resources. If no source network is specified, the default value of this field is **Any**. For reverse connections, this option can be used to block access requests to users' computers that originate from specific ports or application resources.

6. Use **Destination restrictions** to restrict access over individual **Ports** or a range of ports. To enable access on any port, click **Any**. To specify multiple ports, click **Selected** and type the port numbers, separated by semicolons. To specify a port range, type the beginning and ending numbers separated by a hyphen. For example, if you are building a policy to control access to an SMTP mail server, you might allow access only over port 25 (the well-known port for SMTP traffic). A list of the latest port number assignments is available at http://www.iana.org/assignments/port-numbers.



DESTINATION RESTRICTIONS

Ports:

● Any ○ Selected

Permissions: ○ Read/Write ● Read

Controls the user's access to file system resources.

Use **Permissions** to specify whether the rule will allow **Read** or **Read/Write** access to the file system resources. These access privileges work in conjunction with Windows access control rules. For a user to have certain file permissions, both entities (that is, Windows and the appliance) must allow them. If you disable file uploads, no user can write to a file, although users with write access will be able to move and delete files. These settings are ignored by reverse connections.

7. Under **Time and date restrictions**, specify when the rule will be in effect. (The time zone for the time restriction fields is your local time.) You can specify a **Shift** or a **Range**, or you can specify that the rule remain in effect at all times.

8. Click **Save** or, if you want to define another rule, click **Finish and Add Another**.

Because AMC gives you the flexibility to assign multiple access methods to resources, situations may arise in which there is a mismatch between access methods and resources. This happens if you create a rule that assigns an access method that is incompatible with the specified resource. For example, designating **Web browser** as the method for accessing a Windows domain resource will trigger an "Invalid destination resources" error message in AMC. For more information, see Resolving Invalid Destination Resources.

In some cases you can create a Deny rule that contains a mix of resources and access methods that may prevent subsequent rules from being evaluated. This could inadvertently block user access to other resources referenced in the access policy. The logic used to determine access method and resource compatibility is described in Resolving Deny Rule Incompatibilities.

Reverse connections are available only when IP address pools are configured for the network tunnel clients. AMC displays an error message if you attempt to change the rule from a forward connection to a reverse connection and no IP address pools are configured.

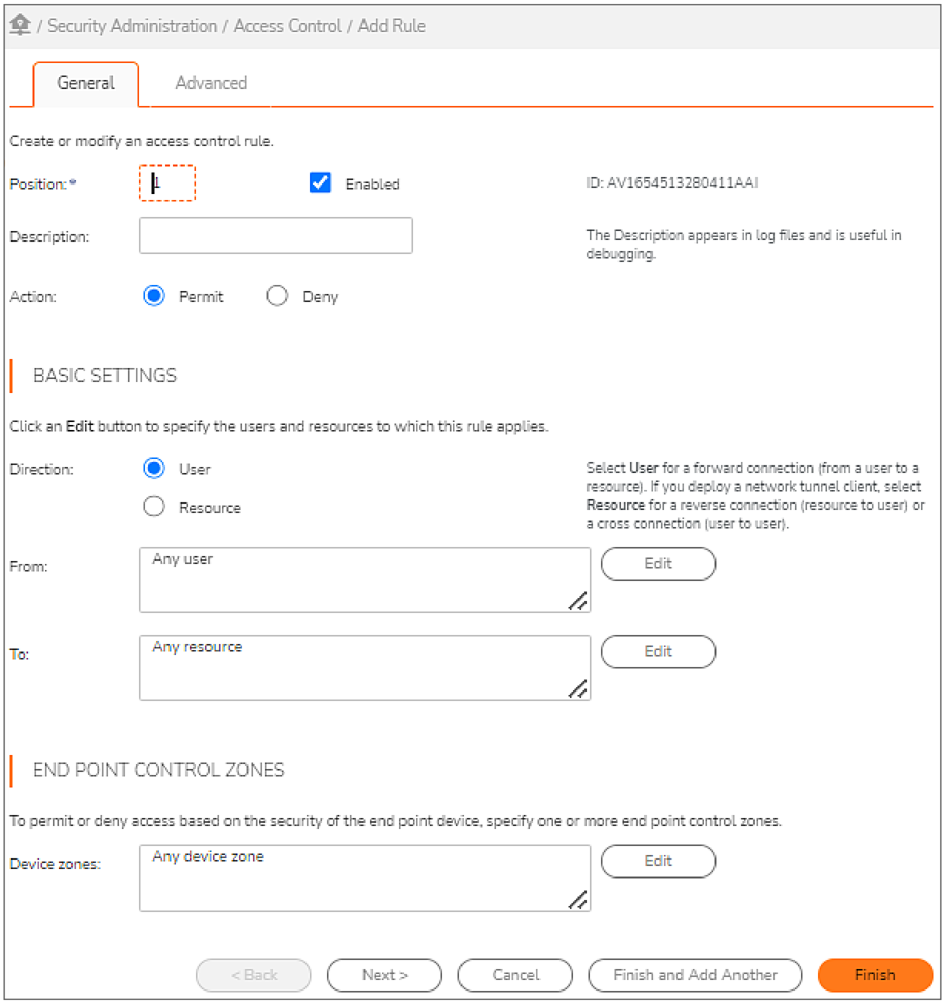
Adding Access Control Rules for a Reverse Connection

Perform the following steps to add an access control rule for a reverse connection from a destination resource to users. Examples of reverse connections include IBM's Tivoli provisioning products, and Microsoft's Systems Management Server (SMS). For more information, see Requirements for Reverse and Cross-Connections.

To add an access control rule for a reverse connection:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon.

   The **Add Access Rule** page displays.



Create or modify an access control rule.

Position:* 1

☑ Enabled

ID: AV1654513280411AAI

Description:

The Description appears in log files and is useful in debugging.

Action: ● Permit ○ Deny

BASIC SETTINGS

Click an **Edit** button to specify the users and resources to which this rule applies.

Direction: ● User ○ Resource

Select **User** for a forward connection (from a user to a resource). If you deploy a network tunnel client, select **Resource** for a reverse connection (resource to user) or a cross connection (user to user).

From: Any user

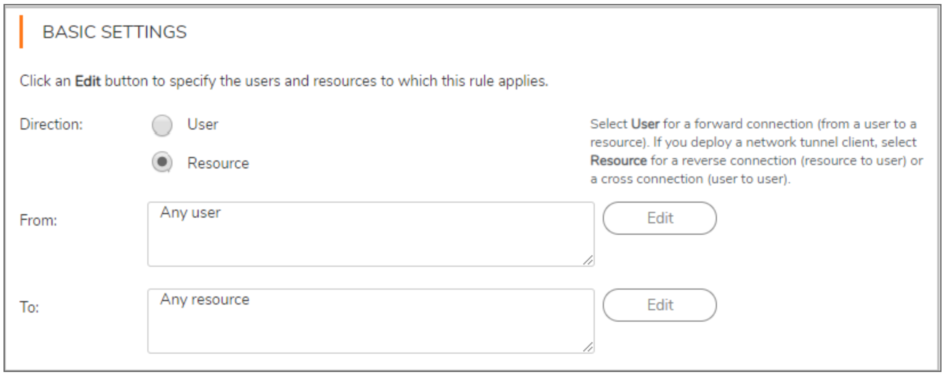
To: Any resource

END POINT CONTROL ZONES

To permit or deny access based on the security of the end point device, specify one or more end point control zones.

Device zones: Any device zone

3. In the **Number** field, type a number to specify the rule's position in the access rule list. By default, new rules are added to the top of the list, but you can use this box to place the rule anywhere you want. For example, if you have four rules and you assign the number `3` to a new one, it is inserted before the current rule 3 (which will become rule 4). This field is required.
4. In the **Description** field, type a descriptive comment about the rule. This step is optional, but a description can be helpful when viewing your list of rules later, and also appears in log files where it is useful in debugging. The **ID** is a unique identifier automatically assigned by AMC; it cannot be edited.
5. Use the **Action** buttons to specify whether the rule will be used to **Permit** or **Deny** access, or if the rule is **Disabled**.
6. Complete the information listed under **Basic settings**:



BASIC SETTINGS

Click an **Edit** button to specify the users and resources to which this rule applies.

Direction: ○ User ● Resource

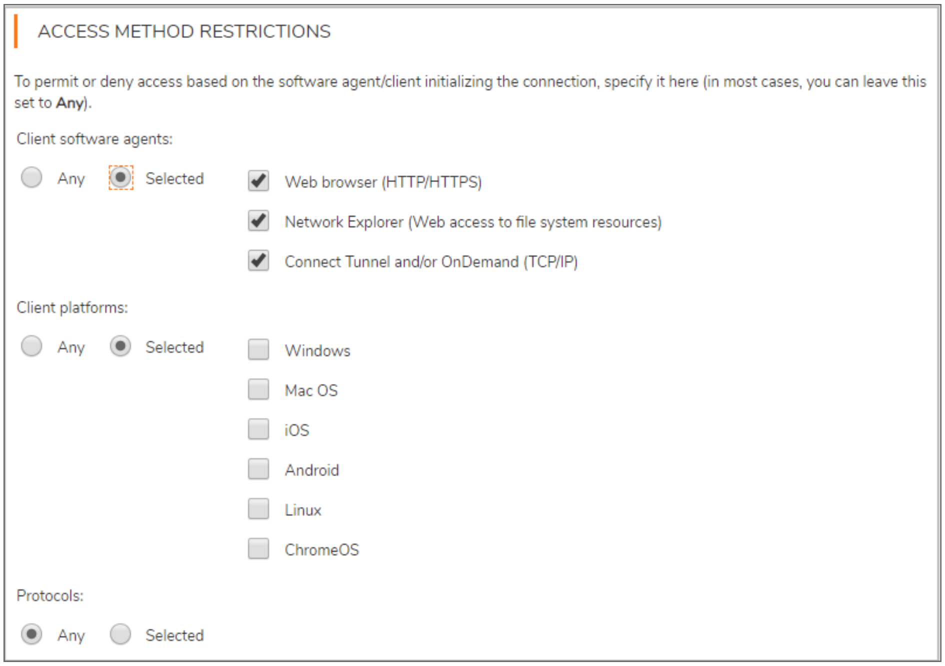
Select **User** for a forward connection (from a user to a resource). If you deploy a network tunnel client, select **Resource** for a reverse connection (resource to user) or a cross connection (user to user).

From: Any user

To: Any resource

   - Select the **Resource** button to create a rule controlling a reverse connection from a resource to a user. The **User** and **Resource** buttons toggle between forward-connection and reverse-connection rules.

     Reverse connections are available only when IP address pools are configured for the network tunnel clients. If you attempt to create a reverse connection with no IP address pools configured, AMC displays an error message. For more information, see Access Control Rules for Bi-Directional Connections.
   - The **From** field specifies the resources that will connect to users. Click **Edit** to select from a list of resources. If no resources are specified, the default value for this field is **Any resource**.
   - The **To** field specifies the users to which the resource will connect. Click **Edit** to select from a list. If no users are selected, the default value for this field is **Any user**.
7. Click **Next** to display the **Advanced** page.
8. In the **Access methods** area, select **Any** to automatically manage access to all resources in the rule regardless of the access method making the request. This ensures that either the Connect Tunnel client or the OnDemand Tunnel agent, which is required for reverse connections, is managed by the rule. The other access methods do not support reverse connections and will be bypassed.



ACCESS METHOD RESTRICTIONS

To permit or deny access based on the software agent/client initializing the connection, specify it here (in most cases, you can leave this set to **Any**).

Client software agents:

○ Any ● Selected

☑ Web browser (HTTP/HTTPS)

☑ Network Explorer (Web access to file system resources)

☑ Connect Tunnel and/or OnDemand (TCP/IP)

Client platforms:

○ Any ● Selected

☐ Windows

☐ Mac OS

☐ iOS

☐ Android

☐ Linux

☐ ChromeOS

Protocols:

● Any ○ Selected

9. Click **Save**.

Adding a Pair of Access Control Rules for a Cross-Connection

Most of the steps involved in creating an access control rule for a cross-connection are the same as those for creating a rule for a forward connection or a reverse connection. However, there are some key differences and requirements.

For example, to permit your VPN users to call each other using a VoIP application, create one rule for your users to connect to an IP address pool on the appliance, and a second rule for the IP address pool to connect to the users.

You would also need to follow this procedure to create a pair of rules to permit bi-directional connections between an FTP server and users.

To add an access control rule for a cross-connection:

1. Ensure that the requirements for configuring a reverse connection are met. For more information, see Requirements for Reverse and Cross-Connections.
2. In the AMC, navigate to **Security Administration > Access Control**.
3. Click the **+** (New) icon.

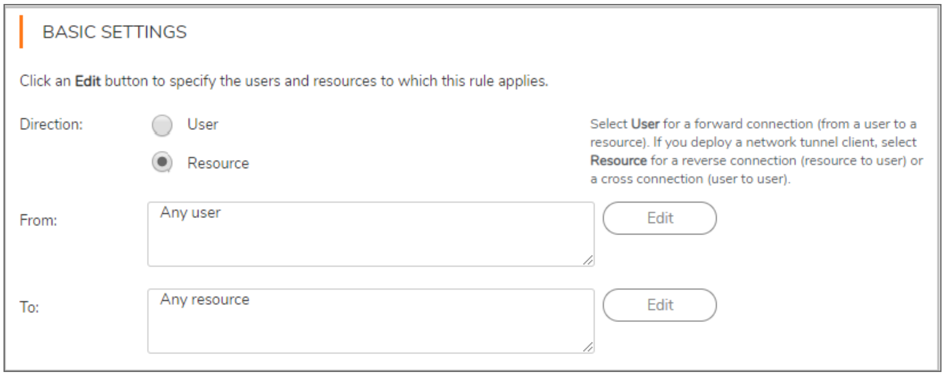
   The **Add Access Rule** page displays.
4. Type a number in the **Position** field to specify the rule’s position in the access rule list. By default, new rules are added to the top of the list, but you can use this box to place the rule anywhere you want. For example, if you have four rules and you assign the number `3` to a new one, it is inserted before the current rule **3** (which will become rule **4**). This field is required.

5. In the **Description** field, type a descriptive comment about the rule. This step is optional, but a description can be helpful when viewing your list of rules later. The description also appears in log files where it is useful when examining logs to determine why a connection did not match a specific rule. The **ID** is a unique identifier automatically assigned by AMC; it cannot be edited.

   Since a cross-connection requires a pair of forward-connection and reverse-connection rules, you should assign similar names to the two rules to make it easy to locate them in the list of access control rules.

6. Use the **Action** buttons to specify whether the rule will be used to **Permit** or **Deny** access, or if the rule is **Disabled**.

7. Under **Basic settings**, use the **User** and **Resource** buttons to select forward-connection or reverse-connection rules.



BASIC SETTINGS

Click an **Edit** button to specify the users and resources to which this rule applies.

Direction: ○ User ● Resource

Select **User** for a forward connection (from a user to a resource). If you deploy a network tunnel client, select **Resource** for a reverse connection (resource to user) or a cross connection (user to user).

From: Any user

To: Any resource

   - To create a forward-connection rule from the users to the IP address pool, click **User**.
   - To create a reverse-connection rule from the IP address pool to the users, click **Resource**.

8. In the **From** field under **Basic settings**, specify the users or resources to which this rule applies:
   - For a forward-connection rule, specify the users or user groups to whom the rule applies. Click **Edit** to select from a list of users or groups. The default value is *Any user*.
   - For a reverse-connection rule, specify the address pool that will be used for the VoIP application. Click **Edit** to select the address pool from a list of resources. The default value is **Any resource**.

9. In the **To** box under **Basic settings**, specify the users or resources to which this rule applies:
   - For a forward-connection rule, specify the address pool that will be used for the VoIP application. Click **Edit** to select the address pool from a list of resources. The default value is **Any resource**.
   - For a reverse-connection rule, specify the users to whom the rule applies. Click **Edit** to select from a list of users or groups. The default value is **Any user**.

10. In the **Access method restrictions** area, select **Any**. This enables the appliance’s Smart Access feature to determine the appropriate access method for the users’ end point devices, which for a reverse connection is either the Connect Tunnel client or the OnDemand Tunnel agent. The other access methods do not support cross-connections or bi-directional connections and will be bypassed.

11. In the **Access method restrictions** area, select **Any** to automatically manage access to all resources in the rule regardless of the access method making the request. This ensures that either the Connect Tunnel client or the OnDemand Tunnel agent, which are required for reverse connections, are managed by the rule. The other access methods do not support reverse connections and will be bypassed.

12. Click **Finish** after you have created the first rule in the pair of cross-connection rule, and then create and save the second rule. (Alternatively, you can save the first rule in the pair, make a copy of it, and then reverse the user and resource settings.)

After you have configured the forward-connection rule and the reverse-connection rule that make up the cross-connection rule pair, you should position the two rules next to each other in the access control list. That will make it easier to identify them as related rules.

AMC displays an error message if you attempt to create a cross-connection rule with no IP address pools configured. For more information, see Access Control Rules for Bi-Directional Connections.

Configuring Advanced Access Control Rule Attributes

For most rules, a basic configuration that includes users or groups, destination resources, and access methods is sufficient. Settings that provide even tighter access are available on the **Advanced** page for **Add/Edit Access Rule**.

For example, if you want to restrict connections to those coming from an individual IP address, select the **User's network address** option. Source networks are referenced in an access rule to permit or deny a connection to a destination resource based on the location from which the request originates, which provides you with even greater security.

To configure advanced settings for an access control rule:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the name of an existing rule.
   The **Edit Access Rule** page displays.
3. Click the **Advanced** tab.
4. Under **Access method restrictions**, permit or deny access based on the software agent or client initializing the connection. In most cases, you can leave this set to **Any**.
5. To restrict the **Protocols** that the network tunnel or proxy service will accept from the client, click **Selected**. A brief description of each command is included in the below table, but for more details, see http://www.ietf.org/rfc/rfc1928.txt.

Advanced Access Control Rule Attributes

Protocol	Description
TCP	Enables normal TCP connections (for example, SSH, telnet, SCP, and so forth).
UDP	Allows the network tunnel or proxy service to make a UDP data transfer. This is necessary for operations such as streaming audio and Microsoft Outlook new-mail notification.

ICMP	(Internet Control Message protocol) Enables the ping and traceroute network troubleshooting commands. Selecting this option will configure the network tunnel or proxy service to allow these operations on your behalf. This option also enables ICMP packets to flow through the network tunnel or proxy service.
Accept bind requests from server	Used in protocols that require the client to accept connections from the server. FTP is a notable example: bind usually occurs with a Connect/Bind pair of connections.

6. Specify the names of any source networks you want evaluated in the rule with the **User's network address option**. This is useful for controlling access based on the origin of the connection request. Click **Edit** to select from the list of resources. If no source network is specified, the default value of this field is *Any*. For reverse connections, this option can be used to block access requests to users' computers that originate from specific ports or the application resources.
7. Use **Destination restrictions** to restrict access over individual **Ports** or a range of ports. For example, if you are building a policy to control access to an SMTP mail server, you might allow access only over port 25 (the well-known port for SMTP traffic). A list of the latest port number assignments is available at http://www.iana.org/assignments/port-numbers.

   To enable access on any port, click **Any**. To specify multiple ports, click **Selected** and type the port numbers, separating each with a semicolon. To specify a port range, type the beginning and ending numbers separated by a hyphen.
8. Use **Permissions** to specify whether the rule will allow **Read** or **Read/Write** access to the file system resources. These access privileges work in conjunction with Windows access control rules. For a user to have certain file permissions, both entities (that is, Windows and the appliance) must allow them. If you disable file uploads, no user can write to a file, although users with write access will be able to move and delete files. These settings are ignored by reverse connections.
9. Under **Time and date restrictions**, specify when the rule will be in effect. (The time zone for the time restriction fields is your local time.) You can specify a **Shift** or a **Range**, or you can specify that the rule remain in effect at all times.
10. Click **Save**.

Access Methods and Advanced Options

When you restrict your access methods, the advanced options are enabled or disabled based on which ones remain selected (if you select **Any** as the access method, all the advanced options are available). When AMC validates the rule it prevents you from selecting rule attributes that are not relevant to the access methods. The below table shows the advanced options that apply to each access method.

Access Method Advanced Options

Access method	Applicable advanced options
Web browser (HTTP/HTTPS)	• User's network address • Time and date restrictions

Network Explorer (Web access to file system resources)	• User’s network address • Read/write permissions • Time and date restrictions
Connect Tunnel and/or OnDemand (TCP/IP)	• Protocols • User’s network address • Destination restrictions (ports) • Time and date restrictions

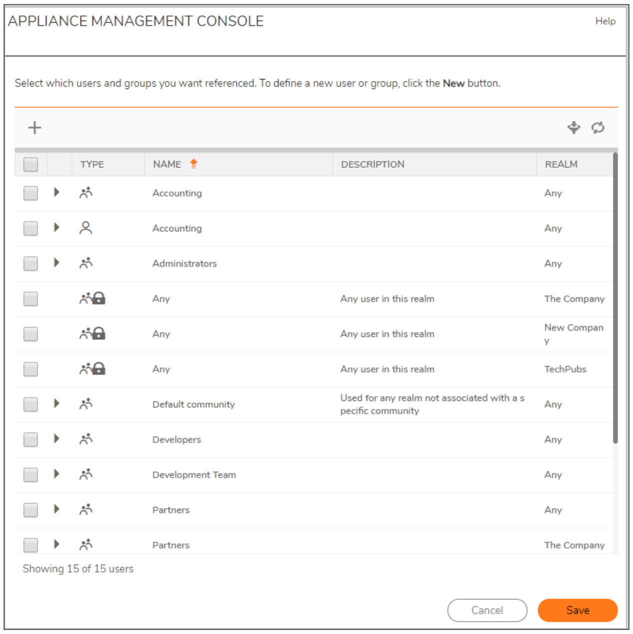
Adding Users and Resources From Within Access Control Rules

Some administrators prefer to define all policy objects (users, groups, and resources) before creating access control rules. Although this structured approach works particularly well for the initial configuration, you may find it inconvenient for ongoing management. If so, you can define new resources directly from the interface used to create access control rules.

To add a user or resource to an existing access control rule:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the name of an existing rule.

   The **Edit Access Rule** page displays.
3. In the **Basic settings** area, click **Edit** beside the **From** field. A separate page displays displaying your current users and groups. For the meaning of the icons, see the below table.



APPLIANCE MANAGEMENT CONSOLE

Select which users and groups you want referenced. To define a new user or group, click the **New** button.

□	TYPE	NAME	DESCRIPTION	REALM
□		Accounting		Any
□		Accounting		Any
□		Administrators		Any
□		Any	Any user in this realm	The Company
□		Any	Any user in this realm	New Compan y
□		Any	Any user in this realm	TechPubs
□		Default community	Used for any realm not associated with a s pecific community	Any
□		Developers		Any
□		Development Team		Any
□		Partners		Any
□		Partners		The Company

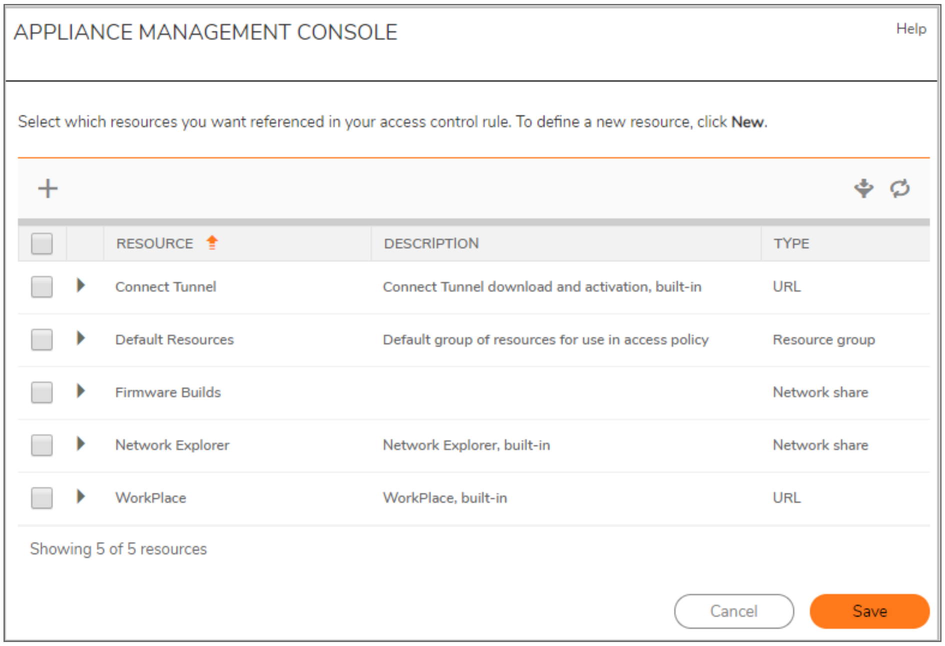
Showing 15 of 15 users

Icon Descriptions

Icon	Description
👥	Community
👥🔒	Any user belongs to the specific realm
👤	User or local user

4. In the **Basic settings** area, click **Edit** beside the **To** field.

   A separate page displays displaying your resources and resource groups.



APPLIANCE MANAGEMENT CONSOLE

Select which resources you want referenced in your access control rule. To define a new resource, click **New**.

□		RESOURCE	DESCRIPTION	TYPE
□	▸	Connect Tunnel	Connect Tunnel download and activation, built-in	URL
□	▸	Default Resources	Default group of resources for use in access policy	Resource group
□	▸	Firmware Builds		Network share
□	▸	Network Explorer	Network Explorer, built-in	Network share
□	▸	WorkPlace	WorkPlace, built-in	URL

Showing 5 of 5 resources

5. Click the **+** (New) icon.

   The page displayed next depends on the type of object you are creating.

6. Define the settings for the new user, group, or resource.

7. Click **Save**.

8. Select the checkbox beside the object you want to add to the access rule and then click **Save**.

Editing, Copying, and Deleting Access Control Rules

Before modifying or deleting an access control rule, carefully examine your existing rules to understand how your changes will affect your security policy.

△ | **CAUTION: Use caution when deleting rules because you are not prompted to confirm the deletion.**

- You can reorder the placement of rules in the access control list. But before you do any reordering, carefully examine them to understand how the new order will affect your security policy.

- Rather than creating a new access control rule from scratch, you can save time by making a copy of an existing rule and changing some parameters to fit the new rule. Choose a rule that shares characteristics with the rule you plan to create.

  Copying is also useful when experimenting with a new access rule: you can edit the copied rule and disable the original rule during your testing. This way you can roll back to your original rule if necessary.

For more information on editing, deleting, and copying access control rules, see Deleting Referenced Objects.

When you use the **Filters** settings to filter the view of the access rules by a specific access method or other criteria, you cannot use the **Move Up** and **Move Down** buttons to reorder the list. You can move an access control rule only when **Method** is set to **All**.

To move a rule more than one position in the list, it's usually faster to change the **Number** box on the **Add/Edit Access Rule** page.

Resolving Deny Rule Incompatibilities

In a Permit rule, you can safely mix and match resources and access methods. However, Deny rules containing specific combinations of resources and access methods may prevent subsequent rules from being evaluated. This can inadvertently block user access to resources referenced later in your access policy.

During its policy evaluation, the appliance may in some cases be unable to determine whether a Deny rule matches an incoming connection request. As a security precaution, it stops processing your rule set and blocks user access.

If you attempt to define a Deny rule referencing any of the three combinations described in the following table, AMC displays this warning message:

“Some of the resources in this rule are not supported by the selected access method(s), which could inadvertently deny access to some resources.”

The below table lists the rule combinations that trigger the warning.

Rule Incompatibilities

Rule action	Resource type	Access methods
Deny	Windows domain	• Any • Connect and OnDemand • WorkPlace
Deny	URL	• Any • Connect and OnDemand
Deny	File share	• Any • Connect and OnDemand

Example

Suppose you create a Deny rule blocking access to a Windows domain and you leave **Access methods** set to *Any*. A Windows domain is accessible from WorkPlace, so when the appliance receives a connection attempt from WorkPlace, it matches the rule and denies access.

However, if the user makes a connection request from Connect or OnDemand, the appliance is unable to determine whether the Windows domain rule matches the request (regardless of which destination resource is requested). The appliance then stops evaluating any further rules in your policy and immediately denies access. If the Windows domain rule is at the top of your access control rule list, it prevents the user from accessing any VPN resources. And if the next rule in the list is a Permit rule allowing the user to access a VPN resource, it is not evaluated.

Resolving the Problem

To resolve rule incompatibilities, modify the rule so it doesn't reference indeterminate access methods. In the case of a Windows domain or network share, select **Network Explorer** as the only access method. For a URL, select only **Web browser or Connect Tunnel and/or OnDemand Mapped Mode**.

Resolving Invalid Destination Resources

If you attempt to create a rule that assigns an access method to an incompatible destination resource, AMC prevents the conflict and displays an `Invalid resources` warning.

The below table lists the access method/destination resource combinations that trigger this warning.

Invalid Access Method/destination Resource Combinations

Access method	Invalid destination resource
Web browser	• Windows domain • Network share
Network Explorer	• URL (and Matching URL)
Connect or OnDemand	• URL (and Matching URL) • Windows domain

Invalid Resource Examples

AMC will not permit you to save a rule that contains a method/resource conflict: if you click **Save**, AMC removes the invalid resource from the rule. If the rule contains only one mismatched resource, it is replaced with **Any**. Examples of method/resource conflict are:

- If a rule specifies **Web browser** as the *only* available access method, it cannot refer to a Windows domain resource. (A Windows domain resource is one that has **Domain** as its type, and for which the **Windows domain** check box is selected).
- A rule that specifies a **Matching URL** resource requires **Web browser** as an access method; if the allowed access methods for a rule don't include **Web browser**, the `Invalid resource` warning appears.

To resolve a destination resource error, modify the rule so that the type of access method is compatible with the destination resource. The simplest way to avoid an access method/destination resource conflict is to remove any **Access method restrictions** on the **Advanced** tab of the **Add/Edit Access Rule** page by leaving both **Client software agents** and **Protocols** set to **Any**.

System Administration

Topics:

Optional Network Configuration

This section describes how to configure and use system logging and monitoring, and how to configure Secure Sockets Layer (SSL) encryption options. It also describes how to use a variety of tools to upgrade, roll back, or reset software versions and to back up or reset configuration files.

It explains how to enable SSH access from remote hosts, and how to enable Internet Control Message Protocol (ICMP) so you can ping the appliance. It also describes how to configure the time settings on the appliance.

For information about configuring and using SNMP, see SNMP Configuration.

Topics:

Enabling SSH Access from Remote Hosts

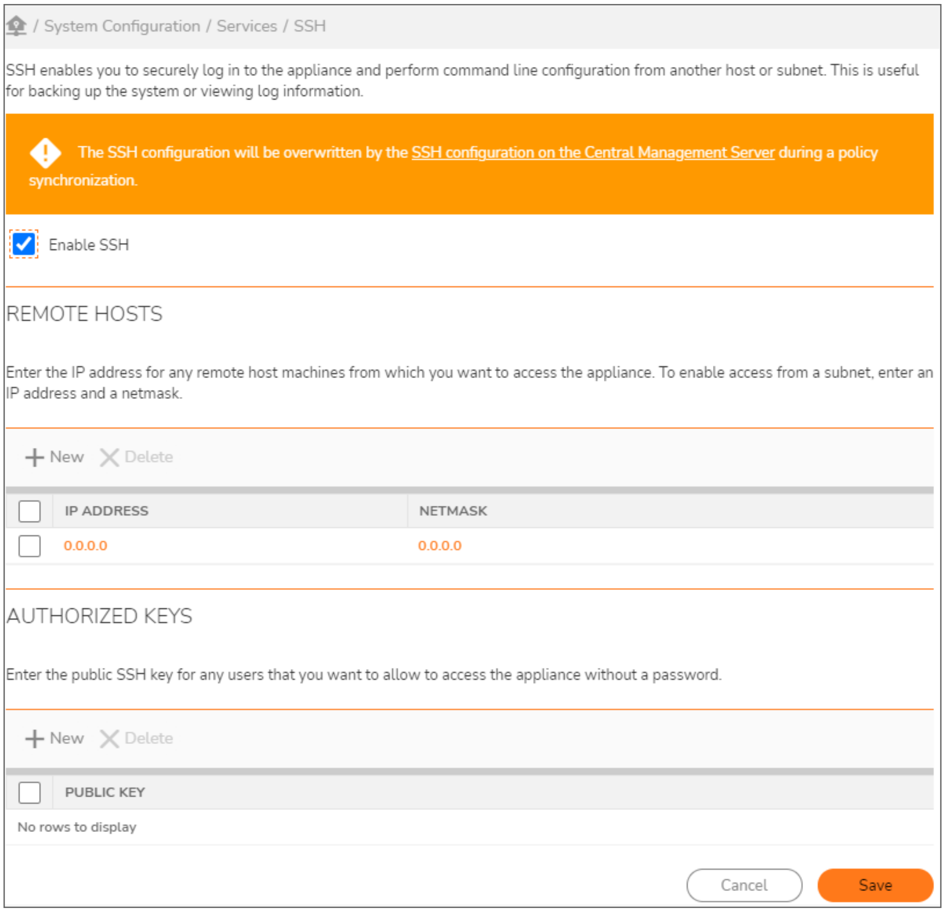
Enabling SSH provides an easy way to access the appliance console from another system. You can enable SSH access from your internal or external network. The local SSH server daemon (sshd) listens on port 22 (the well-known port number for SSH).

The default login grace time is now set as 60 seconds, which is a recommended security practice and federal certification requirements.

To enable SSH access:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Network Services** section, click the **Configure** link under **SSH**.

3. To enable SSH, select the **Enable SSH** check box.



/ System Configuration / Services / SSH

SSH enables you to securely log in to the appliance and perform command line configuration from another host or subnet. This is useful for backing up the system or viewing log information.

The SSH configuration will be overwritten by the SSH configuration on the Central Management Server during a policy synchronization.

☑ Enable SSH

REMOTE HOSTS

Enter the IP address for any remote host machines from which you want to access the appliance. To enable access from a subnet, enter an IP address and a netmask.

□	IP ADDRESS	NETMASK
□	0.0.0.0	0.0.0.0

AUTHORIZED KEYS

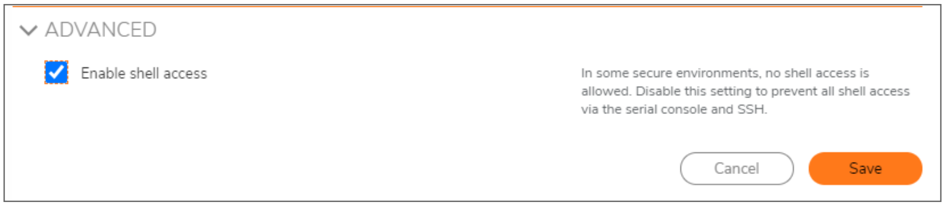
Enter the public SSH key for any users that you want to allow to access the appliance without a password.

□	PUBLIC KEY
No rows to display	

4. To add a host from which you want to enable SSH access, click **+** icon, type the IP address and subnet mask for the host you want to add, and then click **OK**.

5. To add a authorized key for users that you want to allow to access the appliance without a password, click **+** icon, paste the public SSH key, and then click **OK**.

6. In **Advanced** section you can enable or disable the shell access.



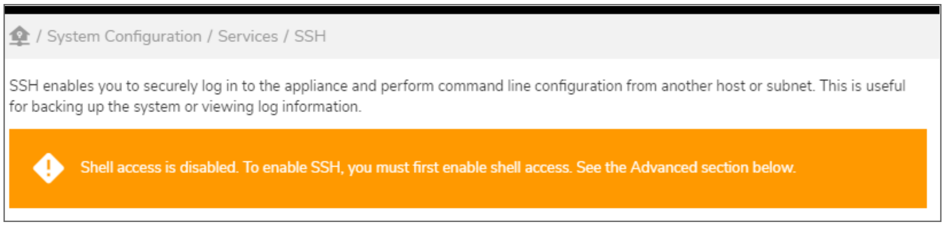
ADVANCED

☑ Enable shell access

In some secure environments, no shell access is allowed. Disable this setting to prevent all shell access via the serial console and SSH.

ⓘ **NOTE:** If your network does not allow shell access then clear the **Enable shell access** check box. When the **Enable shell access** check box is cleared, the **Enable SSH** check box is also cleared and disabled. This prevents all shell access via the serial console and SSH.

ⓘ **NOTE:** The following warning message is displayed.



SSH enables you to securely log in to the appliance and perform command line configuration from another host or subnet. This is useful for backing up the system or viewing log information.

Shell access is disabled. To enable SSH, you must first enable shell access. See the Advanced section below.

7. Click **Save**.

To delete a host:

1. Select any hosts you want to remove.
2. Click **Delete**
3. Click **Save**.

ⓘ **NOTE:** You can enable SSH access from any host by typing 0.0.0.0 for both the IP address and the subnet mask. Keep in mind, however, that the trade-off for this convenience is decreased appliance security.

To delete a public SSH key:

1. Select the check box to left of any public key you want to remove.
2. Click **Delete** icon, and then click **Save**.

Configuring ICMP

Enabling ICMP allows you to use the ping command to test network connectivity to the appliance from another computer on the same subnet. This will not enable broadcast pings.

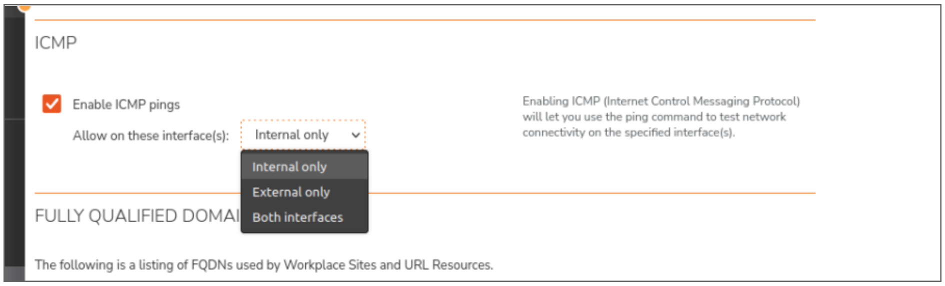
△ **CAUTION: Enabling ICMP makes it possible to ping the appliance from both network interfaces (external and internal). Unless you suppress ICMP Echo Request traffic using a firewall or other network device, it will be possible to discover the appliance from the Internet.**

From 12.4.2 onwards in AMC/CMC you can select multiple interface option for ICMP for internal only or external only or both interfaces.

To enable ICMP:

1. In the AMC, navigate to **System Configuration > Network Settings**.
2. In the **Basic** section, click the **Edit** link.

   The **Basic Network Settings** page displays.
3. In the **ICMP** section, select the **Enable ICMP pings** check box.
4. In **Allow on these interface(s)**, select any of the following:
   - **Internal only**
   - **External only**
   - **Both Interfaces**



ICMP

☑ Enable ICMP pings

Allow on these interface(s): Internal only

Enabling ICMP (Internet Control Messaging Protocol) will let you use the ping command to test network connectivity on the specified interface(s).

FULLY QUALIFIED DOMAI

The following is a listing of FQDNs used by Workplace Sites and URL Resources.

5. Click **Save**.

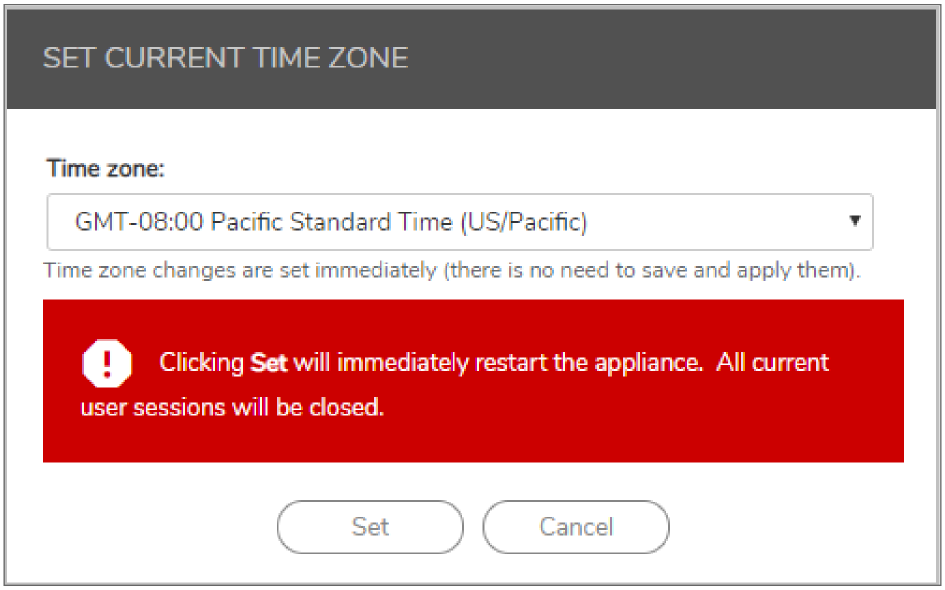
Configuring Time Settings

ⓘ **IMPORTANT:** Changing the time or time zone immediately restarts the appliance. All current user sessions will be closed.

To set the date and time referenced on the appliance and in system logs, select a time zone and then set the local time, if necessary. There are two ways to set the current time: manually, or by synchronizing with one or more Network Time Protocol (NTP) servers.

To change the time zone:

1. In the AMC, navigate to **System Configuration > General Settings**.
2. In the **Appliance Options** section, click **Edit**.
3. In the **Date/time** area, click **Change** for **Time zone**.
   The **Set Current Time Zone** dialog displays.



SET CURRENT TIME ZONE

Time zone:

GMT-08:00 Pacific Standard Time (US/Pacific)

Time zone changes are set immediately (there is no need to save and apply them).

Clicking **Set** will immediately restart the appliance. All current user sessions will be closed.

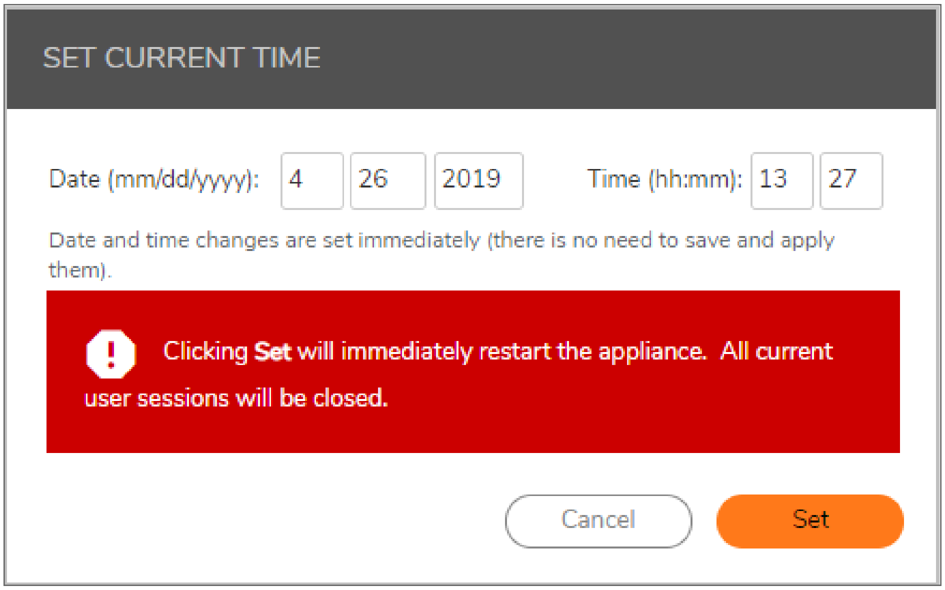
4. Select your current local time zone from the **Time zone** drop-down menu, which shows the time as Greenwich Mean Time (GMT).
5. Apply your pending changes.

To manually configure the system time:

> ⓘ **NOTE:** If you are using a SonicWall-provided evaluation license, do not move your system time backward from the current time; doing so will disable all services on your appliance for licensing reasons.

1. In the AMC, navigate to **System Configuration > General Settings**.
2. In the **Appliance Options** section, click **Edit**.
3. In the **Date/time** area, click **Change** for **Current system time**.

   The **Set Current Time** dialog displays.



SET CURRENT TIME

Date (mm/dd/yyyy): 4 26 2019 Time (hh:mm): 13 27

Date and time changes are set immediately (there is no need to save and apply them).

Clicking **Set** will immediately restart the appliance. All current user sessions will be closed.

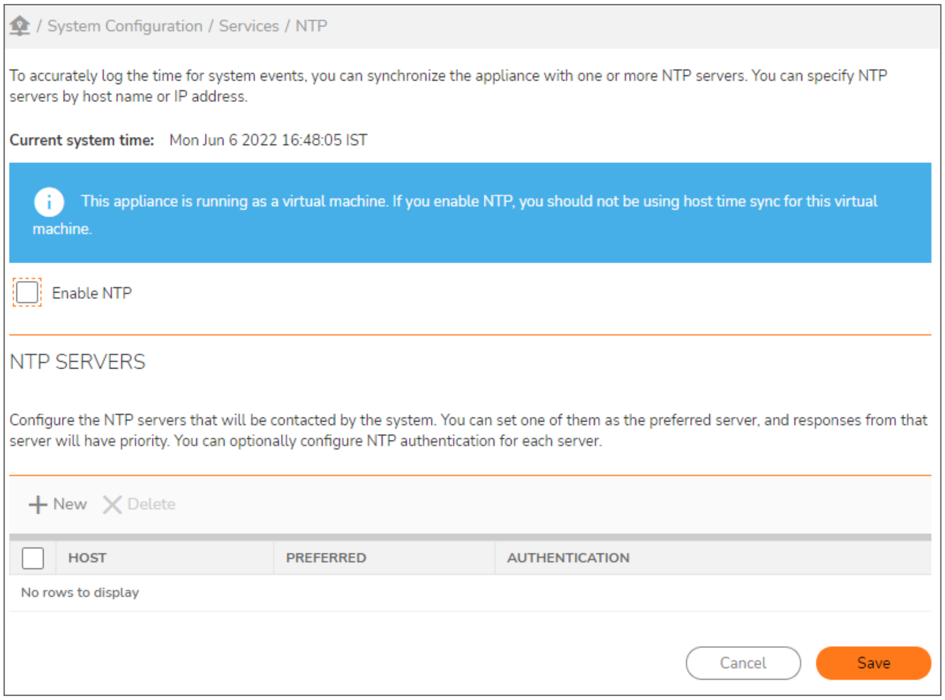
4. Enter the current date and time and click **Set**to apply your changes immediately.

To configure the system time using NTP:

To accurately log the time for system events, you can synchronize the appliance with one or more NTP servers. You can specify NTP servers by host name or IP address. The appliance can use NTP authentication keys, making it impossible for someone to spoof an NTP server and update the appliance with incorrect time settings. We recommend that you synchronize only with NTP servers on your internal network.

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Network Services** section, click the **Configure** link under **NTP**.

   The **NTP Settings** page displays.



/ System Configuration / Services / NTP

To accurately log the time for system events, you can synchronize the appliance with one or more NTP servers. You can specify NTP servers by host name or IP address.

Current system time: Mon Jun 6 2022 16:48:05 IST

This appliance is running as a virtual machine. If you enable NTP, you should not be using host time sync for this virtual machine.

□ Enable NTP

NTP SERVERS

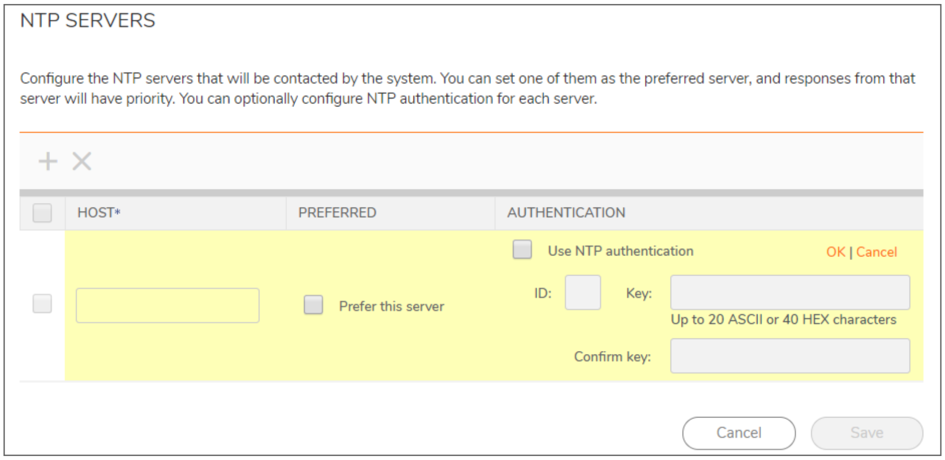
Configure the NTP servers that will be contacted by the system. You can set one of them as the preferred server, and responses from that server will have priority. You can optionally configure NTP authentication for each server.

□	HOST	PREFERRED	AUTHENTICATION

No rows to display

3. To enable NTP, select the **Enable NTP** check box.

4. Under the NTP Servers, click on + icon.



NTP SERVERS

Configure the NTP servers that will be contacted by the system. You can set one of them as the preferred server, and responses from that server will have priority. You can optionally configure NTP authentication for each server.

□	HOST*	PREFERRED	AUTHENTICATION
□		□ Prefer this server	□ Use NTP authentication OK | Cancel ID: Key: Up to 20 ASCII or 40 HEX characters Confirm key:

5. In the **Host** field, enter the URL or IP address of NTP server which you want to synchronize your appliance.

6. Click **Prefer this server** check box to set the NTP server as preferred server and responses from this server will have high priority. In addition, selecting this option will unselect all other NTP servers and responses from the servers will have less priority. Only one host can be marked as preferred server.

   ⓘ **NOTE:** When you are upgrading from prior version of SMA to 12.4, the server which you have configured as primary server is set as the preferred server by default.

7. Optionally, click **Use NTP authentication** check box if you want to configure authentication for each server. Authenticated NTP is a standard feature of NTP protocol that allows basic validation of the identity of an NTP server using a shared key. This option prevents the user from modifying the timestamps.

   ⓘ | **NOTE:** Contact your system administrator for the authentication ID and Key. In the current release, only SHA1 hash algorithm is supported and MD5 is not supported.

8. Click **OK**.

9. Click **Save**.

ⓘ | **NOTE:** You can add up to four NTP servers by clicking on + icon.

System Logging and Monitoring

The SMA appliance logs a variety of useful information, including user access, system events, and changes in AMC. This section explains how to configure and view logs in AMC, and how to send messages to an external syslog server. It also describes the system status information displayed by AMC.

If a central syslog server is not available, you can review log files from the command-line interface on the appliance itself using standard UNIX commands. For information on how to manually view and interpret raw log data, see Log File Output Formats.

Topics:

- Overview: System Logging and Monitoring
- Log Files
- Monitoring the Appliance
- SNMP Configuration

Overview: System Logging and Monitoring

The appliance logs data for the operation of AMC and the services on the appliance; it also collects data on how administrators have used and changed the system. All system logs are collected and stored in the syslog format, and log messages are handled using an updated version of the standard syslog format.

The appliance is initially configured to store log files locally. If you configure it to send log files to a central syslog server, you can monitor system-level events in near real time, and receive notifications about significant events. You can also export log message data to a comma-separated values (`.csv`) file for viewing and analysis with other applications.

Log Files

The appliance generates several types of log files that can be viewed and exported from the **Logging** page in AMC. There are also two log files related to WorkPlace that can’t be viewed in AMC; they are described in WorkPlace Logs.

Topics:

- Viewing Logs
- Sorting, Searching, and Filtering Log Messages
- Exporting Log Files
- Configuring Log Settings
- System Message Log
- Management Message Log
- Management Audit Log
- Network Tunnel Audit Log
- Web Proxy Audit Log
- Client Installation Logs (Windows)

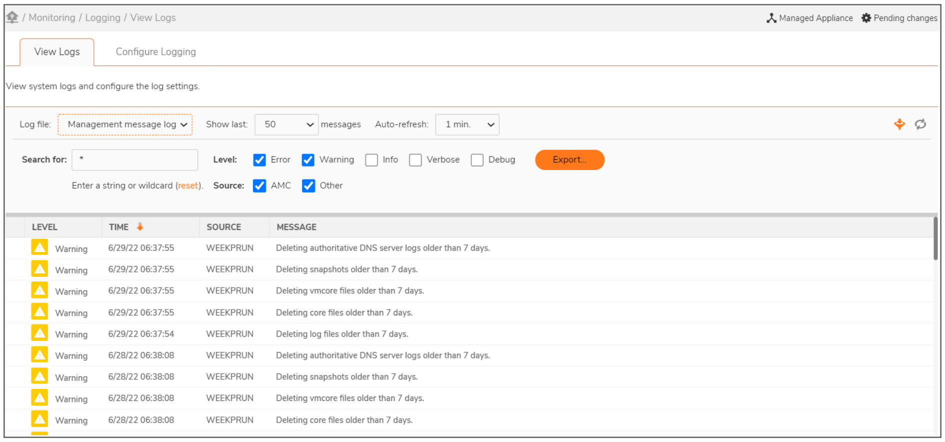
Viewing Logs

There are several log files generated by the SMA appliance, and AMC enables you to sort, search, and filter them.

To view logs:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.



View system logs and configure the log settings.

Log file: Management message log | Show last: 50 messages | Auto-refresh: 1 min.

Search for: * | Level: ☑ Error ☑ Warning □ Info □ Verbose □ Debug

Enter a string or wildcard (reset). | Source: ☑ AMC ☑ Other

LEVEL	TIME	SOURCE	MESSAGE
Warning	6/29/22 06:37:55	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/29/22 06:37:55	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/29/22 06:37:55	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/29/22 06:37:55	WEEKPRUN	Deleting core files older than 7 days.
Warning	6/29/22 06:37:54	WEEKPRUN	Deleting log files older than 7 days.
Warning	6/28/22 06:38:08	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/28/22 06:38:08	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/28/22 06:38:08	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/28/22 06:38:08	WEEKPRUN	Deleting core files older than 7 days.

2. Select the system or service log file you want to view from the **Log file** drop-down menu. The columns of information displayed are different for each type of log file, as described in the below table.

   Log File Descriptions

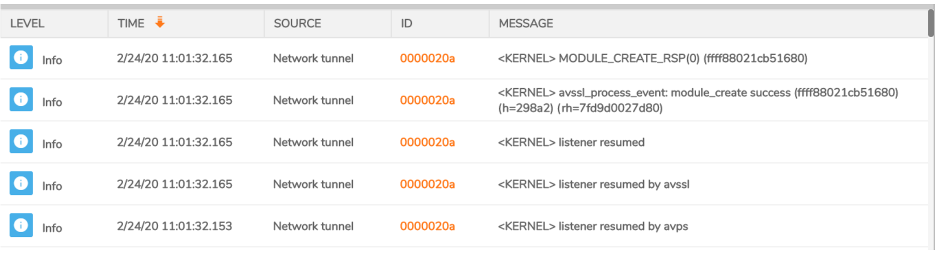
Log file	Description

System message log	Displays server processing and diagnostic information about the network tunnel service and the Web proxy service. It also provides detailed messages about all access control decisions: each time a user request matches a policy rule, a log file entry is recorded explaining the action taken. For details, see System Message Log.
Management message log	Displays entries regarding the operation of AMC, including when the console was started and stopped, and what errors occurred during administration of the appliance. For details, see Management Message Log.
Management audit log	Displays an audit history of configuration changes made in AMC by administrators, showing when changes were made and by which administrator. For details, see Management Audit Log.
Network proxy/tunnel audit log Web proxy audit log	There are two access service audit logs: one for the Web proxy service (called **Workplace** in the log files), and one that combines messages from both the network proxy and network tunnel services (called **Anywhere VPN** in the log files). These two logs provide detailed information about connection activity, including a list of users and the amount of data transferred. For details, see Network Tunnel Audit Log and Web Proxy Audit Log.
Client installation logs	If something goes wrong during client or agent installation on a computer running Windows, the error is recorded in a client installation log. These logs are automatically uploaded to the appliance and listed in AMC if the user has Secure Endpoint Manager installed. For details, see Client Installation Logs (Windows).

Unregistered device log	Displays a list of login attempts from users on devices that are not registered. You can export the list to an XML format that can be used to register these devices.

3. Use the **Show last** drop-down menu to select the number of log messages you want to display. You can choose **50** (default), **100**, **250**, **500**, or **1000** messages.
4. Click the **Refresh** button to update the page to show the most recent log messages, or to view the results of any filtering selections you've made.

   By default, the log viewer's **Auto-refresh** option is set to **1 min**. You can optionally set the refresh time to **30 sec**., **5 min**., **10 min**., **15 min**., or turn it **Off** during your AMC session.
5. Use the optional **Search for** and **Level**, **Source**, and **Status** sorting options to find log messages that meet specific criteria. See Sorting, Searching, and Filtering Log Messages.
6. Click (**>**) in the first column when a log entry is more than a few lines long: click it to expand the entry.



LEVEL	TIME	SOURCE	ID	MESSAGE
Info	2/24/20 11:01:32.165	Network tunnel	0000020a	<KERNEL> MODULE_CREATE_RSP(0) (ffff88021cb51680)
Info	2/24/20 11:01:32.165	Network tunnel	0000020a	<KERNEL> avssl_process_event: module_create success (ffff88021cb51680) (h=298a2) (rh=7fd9d0027d80)
Info	2/24/20 11:01:32.165	Network tunnel	0000020a	<KERNEL> listener resumed
Info	2/24/20 11:01:32.165	Network tunnel	0000020a	<KERNEL> listener resumed by avssl
Info	2/24/20 11:01:32.153	Network tunnel	0000020a	<KERNEL> listener resumed by avps

Sorting, Searching, and Filtering Log Messages

The AMC log viewer allows you to customize the display of log message data using sorting, searching, and filtering options. You can use these options separately or in any combination.

Topics:

- Sorting
- Filtering
- Searching

Sorting

Data displayed in each of the columns in the log table can be sorted in ascending or descending order by clicking the column heading. By default, log messages are sorted by the **Time** column, with the most recent messages shown at the top.

Filtering

With the filtering options, you can include or exclude certain types of logging data for each log file. For example, if you want to see Management message log entries that are not AMC-related (such as system control authority messages), select all of the **Level** check boxes and make sure the **AMC** check box under **Source** is cleared. The available options vary depending on the type of log file you are viewing.

Searching

To search for text strings in the log files, such as an IP address or a user ID, type the (case-sensitive) search criteria in the **Search for** field and then click **Refresh** to view the results. You can use the wildcard characters `*` and `?` in your search criteria. To clear the search criteria, click the **reset** link.

When you're viewing a system message log, you can click a session ID number in the **ID** column to automatically search for all log messages that share the same session ID. For information on session ID see the table of field descriptions in System Message Log.

In the Web proxy audit log and the network proxy/tunnel audit log, you can click a user ID in the **Username** column to automatically search for all log messages about a specific user.

Exporting Log Files

If you need to perform additional analysis of the log message data, or display the data differently, you can export selected data to files for use by another application, such as Microsoft Excel (in the case of logs with comma-separated values) or an XML editor (in the case of the log for unregistered devices).

You can reduce the size of the exported file by first applying filter or search criteria. The **Show last <n> messages** setting determines the maximum number of messages included in the exported log file.

To export a log file:

1. In the AMC, navigate to **Monitoring > Logging**.
   The **View Logs** page displays.
2. Use the **Log file** list to select the system or service log file you want to view.
3. Click the **Filter** icon to display the available filters.
4. Apply any filter or search criteria to the log data. See Sorting, Searching, and Filtering Log Messages.
5. Click **Export**.
6. You might be prompted to save or open the file. Click **Save**.
7. In the **Save As** box, browse for the location where the file will be saved, optionally rename the file, and then click **Save**. By default, AMC assigns the file names shown in the below table to the exported files:

   File Names For The Exported Logs

File name	Description
`sysmessage.csv`	System message log
`management.csv`	Management message log
`consoleaudit.csv`	Management audit log
`netaudit.csv`	Network proxy/tunnel audit log
`webaudit.csv`	Web proxy audit log

`UnregisteredDevices.xml`	Log of devices with an equipment ID that is not recognized. For the steps necessary for collecting device identifiers in this log, see Collecting Equipment IDs from Unregistered Devices.

Configuring Log Settings

If you are debugging the system, you can set the message log level for the services in AMC. Additionally, you can configure the appliance to send log files to an external syslog server.

Topics:

- Setting Log Levels
- Sending messages to a syslog server

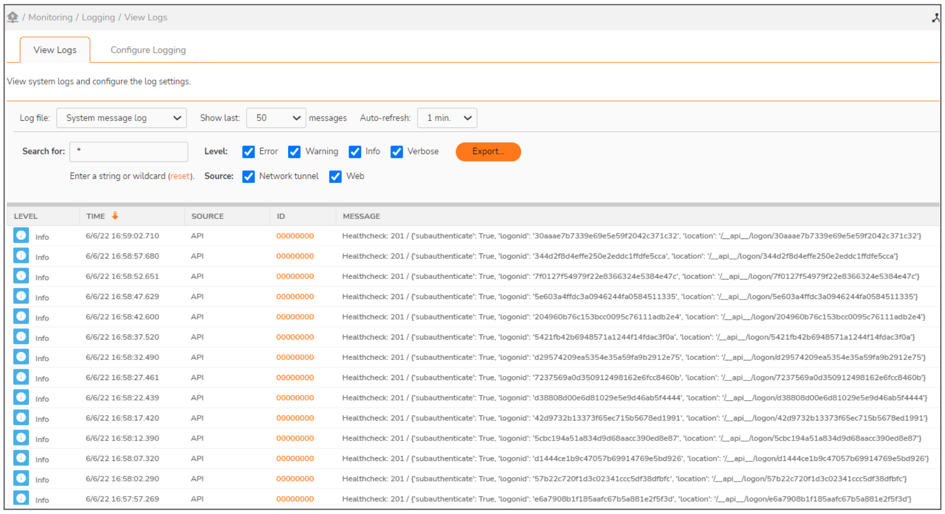
System Message Log

The system message log displays server processing and diagnostic information about the Web proxy service, network proxy, and the network tunnel service. It also provides detailed messages about all access control decisions: each time a user request matches a policy rule, a log file entry is recorded explaining the action taken.

To view the System Message log:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.
2. Select **System message log** from the **Log file** drop-down menu.



View system logs and configure the log settings.

Log file: System message log   Show last: 50 messages   Auto-refresh: 1 min.

Search for: *   Level: ☑ Error ☑ Warning ☑ Info ☑ Verbose   Export...

Enter a string or wildcard (reset).   Source: ☑ Network tunnel ☑ Web

LEVEL	TIME	SOURCE	ID	MESSAGE
Info	6/6/22 16:59:02.710	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '30aaae7b7339e69e5e59f2042c371c32', 'location': '/__api__/logon/30aaae7b7339e69e5e59f2042c371c32'}
Info	6/6/22 16:58:57.680	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '344d2f8d4effe250e2eddc1ffdfe5cca', 'location': '/__api__/logon/344d2f8d4effe250e2eddc1ffdfe5cca'}
Info	6/6/22 16:58:52.651	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '7f0127f54979f22e8366324e5384e47c', 'location': '/__api__/logon/7f0127f54979f22e8366324e5384e47c'}
Info	6/6/22 16:58:47.629	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '5e603a4ffdc3a0946244fa0584511335', 'location': '/__api__/logon/5e603a4ffdc3a0946244fa0584511335'}
Info	6/6/22 16:58:42.600	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '204960b76c153bcc0095c76111adb2e4', 'location': '/__api__/logon/204960b76c153bcc0095c76111adb2e4'}
Info	6/6/22 16:58:37.520	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '5421fb42b6948571a1244f14fdac3f0a', 'location': '/__api__/logon/5421fb42b6948571a1244f14fdac3f0a'}
Info	6/6/22 16:58:32.490	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': 'd29574209ea5354e35a59fa9b2912e75', 'location': '/__api__/logon/d29574209ea5354e35a59fa9b2912e75'}
Info	6/6/22 16:58:27.461	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '7237569a0d350912498162e6fcc8460b', 'location': '/__api__/logon/7237569a0d350912498162e6fcc8460b'}
Info	6/6/22 16:58:22.439	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': 'd38808d00e6d81029e5e9d46ab5f4444', 'location': '/__api__/logon/d38808d00e6d81029e5e9d46ab5f4444'}
Info	6/6/22 16:58:17.420	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '42d9732b13373f65ec715b5678ed1991', 'location': '/__api__/logon/42d9732b13373f65ec715b5678ed1991'}
Info	6/6/22 16:58:12.390	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '5cbc194a51a834d9d68aacc390ed8e87', 'location': '/__api__/logon/5cbc194a51a834d9d68aacc390ed8e87'}
Info	6/6/22 16:58:07.320	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': 'd1444ce1b9c47057b69914769e5bd926', 'location': '/__api__/logon/d1444ce1b9c47057b69914769e5bd926'}
Info	6/6/22 16:58:02.290	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': '57b22c720f1d3c02341ccc5df38dfbfc', 'location': '/__api__/logon/57b22c720f1d3c02341ccc5df38dfbfc'}
Info	6/6/22 16:57:57.269	API	00000000	Healthcheck: 201 / {'subauthenticate': True, 'logonid': 'e6a7908b1f185aafc67b5a881e2f5f3d', 'location': '/__api__/logon/e6a7908b1f185aafc67b5a881e2f5f3d'}

The **View Logs** page displays the information shown in the below table from the system message log file.

System Message Log File Information

Column	Description
Level	Log message detail level: **Fatal**, **Error**, **Warning**, **Info**, **Debug**, or **Verbose**.
Time	Date and time when the message was generated by the service.
Source	Indicates which service generated the message: **Network proxy**, **Network tunnel**, **Web proxy**, or **Policy** server.
ID	The unique ID number assigned to each user session. Click a session ID number to automatically search for all log messages associated with it. For more information on session ID numbers, see System Message Log.
Message	Message text.

ⓘ **NOTE:** For information on manually reviewing log files from the command-line interface on the appliance, see System Message Log.

Management Message Log

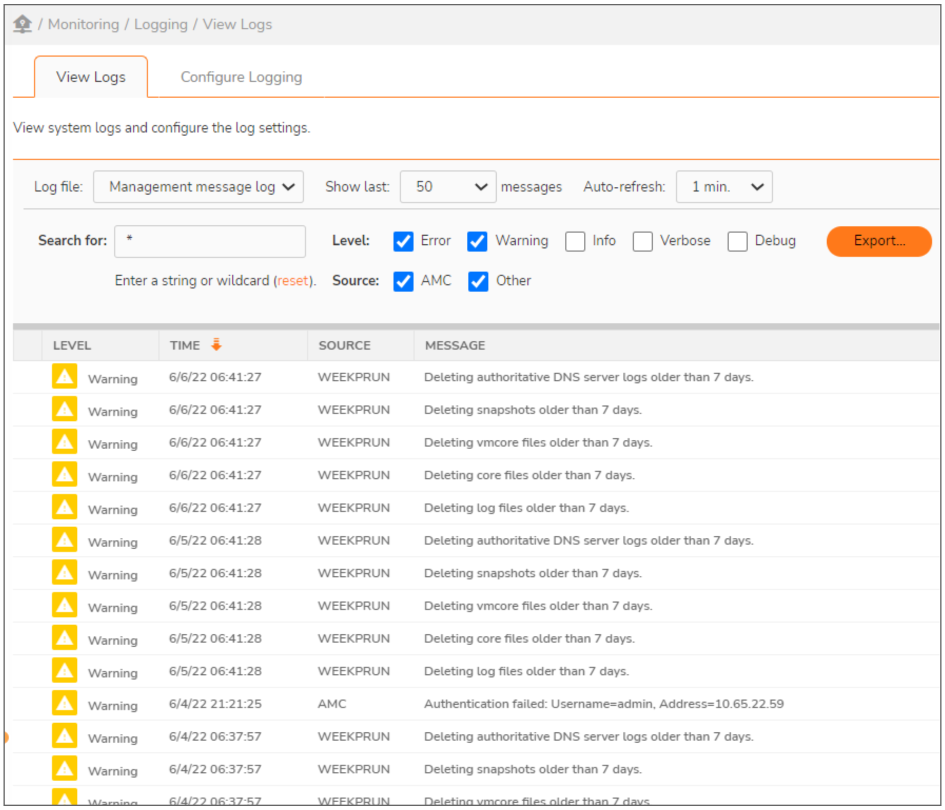
The Management message log contains entries regarding the operation of AMC, including when the console was started and stopped, and what errors occurred during administration of the appliance.

To view the Management Message log:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.

2. Select **Management message log** from the **Log file** drop-down menu.



/ Monitoring / Logging / View Logs

View system logs and configure the log settings.

Log file: Management message log Show last: 50 messages Auto-refresh: 1 min.

Search for: * Enter a string or wildcard (reset).

Level: ☑ Error ☑ Warning □ Info □ Verbose □ Debug

Source: ☑ AMC ☑ Other

LEVEL	TIME	SOURCE	MESSAGE
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting core files older than 7 days.
Warning	6/6/22 06:41:27	WEEKPRUN	Deleting log files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting vmcore files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting core files older than 7 days.
Warning	6/5/22 06:41:28	WEEKPRUN	Deleting log files older than 7 days.
Warning	6/4/22 21:21:25	AMC	Authentication failed: Username=admin, Address=10.65.22.59
Warning	6/4/22 06:37:57	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.
Warning	6/4/22 06:37:57	WEEKPRUN	Deleting snapshots older than 7 days.
Warning	6/4/22 06:37:57	WEEKPRUN	Deleting vmcore files older than 7 days

The **View Logs** page displays the information shown in the below table about the Management message log.

Management Message Log Information

Column	Description
Level	Log message detail level: **Error**, **Warning**, **Info**, **Verbose**, or **Debug**.
Time	Date and time message was logged.
Source	Shows the source for the change: **AMC** or **Other**, which includes *WEEKPRUN* and *sysctrl*.
Message	Describes the log entry in more detail.

Management Audit Log

The Management audit log provides an audit history of configuration changes made in AMC by administrators, showing when changes were made and by which administrator. Configuration changes are either active or pending:

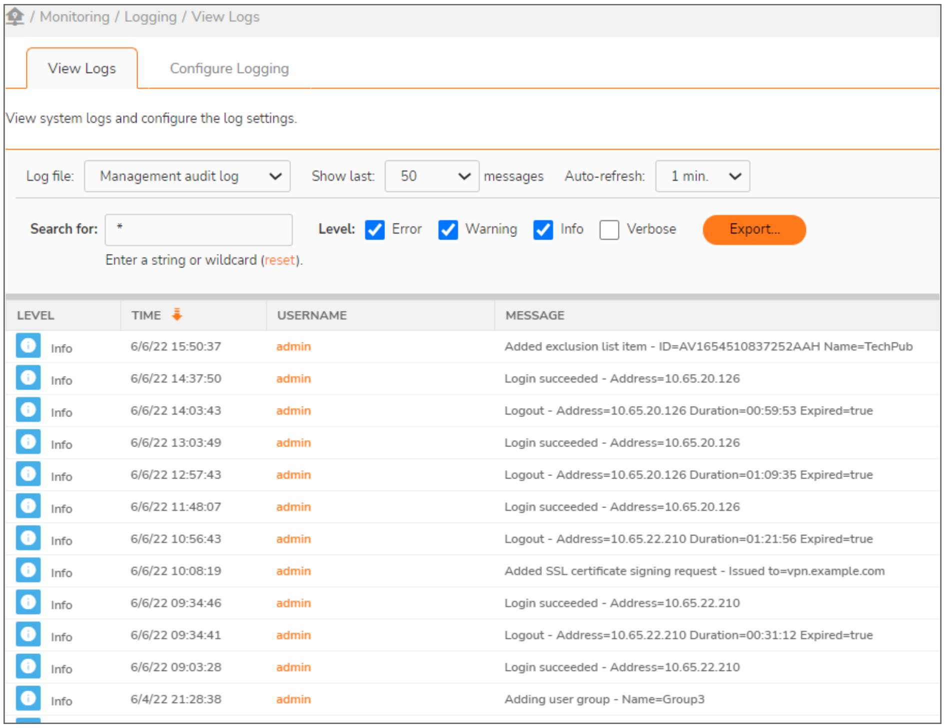
- **Active configuration**: Configuration items that precede the log message `Applied configuration changes` are ones that have been applied and are currently active.

- **Pending changes**: As changes are made, they are saved to disk but not immediately applied. In the Management audit log, these pending changes follow the `Applied configuration changes` message and can be discarded. See Discarding Pending Configuration Changes to find out how to do so.

To view the Management Audit log:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.
2. Select **Management audit log** from the **Log file** drop-down menu.



View system logs and configure the log settings.

Log file: Management audit log

Show last: 50 messages

Auto-refresh: 1 min.

Search for: *

Enter a string or wildcard (reset).

Level: ☑ Error ☑ Warning ☑ Info □ Verbose

LEVEL	TIME	USERNAME	MESSAGE
Info	6/6/22 15:50:37	admin	Added exclusion list item - ID=AV1654510837252AAH Name=TechPub
Info	6/6/22 14:37:50	admin	Login succeeded - Address=10.65.20.126
Info	6/6/22 14:03:43	admin	Logout - Address=10.65.20.126 Duration=00:59:53 Expired=true
Info	6/6/22 13:03:49	admin	Login succeeded - Address=10.65.20.126
Info	6/6/22 12:57:43	admin	Logout - Address=10.65.20.126 Duration=01:09:35 Expired=true
Info	6/6/22 11:48:07	admin	Login succeeded - Address=10.65.20.126
Info	6/6/22 10:56:43	admin	Logout - Address=10.65.22.210 Duration=01:21:56 Expired=true
Info	6/6/22 10:08:19	admin	Added SSL certificate signing request - Issued to=vpn.example.com
Info	6/6/22 09:34:46	admin	Login succeeded - Address=10.65.22.210
Info	6/6/22 09:34:41	admin	Logout - Address=10.65.22.210 Duration=00:31:12 Expired=true
Info	6/6/22 09:03:28	admin	Login succeeded - Address=10.65.22.210
Info	6/4/22 21:28:38	admin	Adding user group - Name=Group3

The **View Logs** page displays the information shown in the below table about the Management audit log.

Management Audit Log Information

Column	Description
Level	Log message detail level: **Fatal**, **Error**, **Warning**, or **Info**.
Time	Date and time of the AMC configuration change.
Username	Shows the name of the administrator as it is configured on the **Manage Administrator Accounts** page.
Message	Shows configuration changes made in AMC.

ⓘ **NOTE:** For information on manually reviewing log files from the command-line interface on the appliance, see Management Console Audit Log.

Network Tunnel Audit Log

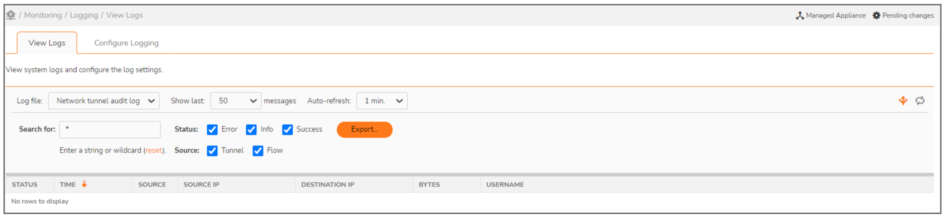
The network proxy/tunnel audit log provides detailed information about connection activity for users who are accessing resources using Connect Tunnel or OnDemand Tunnel, including a list of users and the amount of data transferred.

To view the Network Tunnel Audit log:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.

2. Select **Network tunnel audit log** from the **Log file** drop-down menu.



View system logs and configure the log settings.

Log file: Network tunnel audit log   Show last: 50 messages   Auto-refresh: 1 min.

Search for: *   Enter a string or wildcard (reset).

Status: ☑ Error ☑ Info ☑ Success

Source: ☑ Tunnel ☑ Flow

STATUS	TIME	SOURCE	SOURCE IP	DESTINATION IP	BYTES	USERNAME
No rows to display						

The **View Logs** page displays the information shown in the below table about the network proxy/tunnel audit log file.

Network Proxy/tunnel Audit Log Information

Column	Description
Status	Displays color-coded connection status for each connection request: • Red: Error • Orange: Information • Green: Success When you move the pointer over a connection status code for a specific log message, AMC displays explanatory text below the message.
Time	Date and time of the connection.
Source	Indicates which service generated the message: **Network proxy**, **Network Tunnel**, **Web proxy**, or **Policy** server.
Source IP	The IP address and port number of the computer using the network proxy or tunnel service.
Destination IP	Indicates the IP address and port number of the resource being accessed.
Bytes	Shows three sets of values: • The number of bytes sent • The number of bytes received • The connection duration (in seconds)

Username	The user who requested the resource. You can search for all log messages for a specific user by clicking a username link.

ⓘ **NOTE:** For information on manually reviewing log files from the command-line interface on the appliance, see Network Tunnel Audit Log.

Web Proxy Audit Log

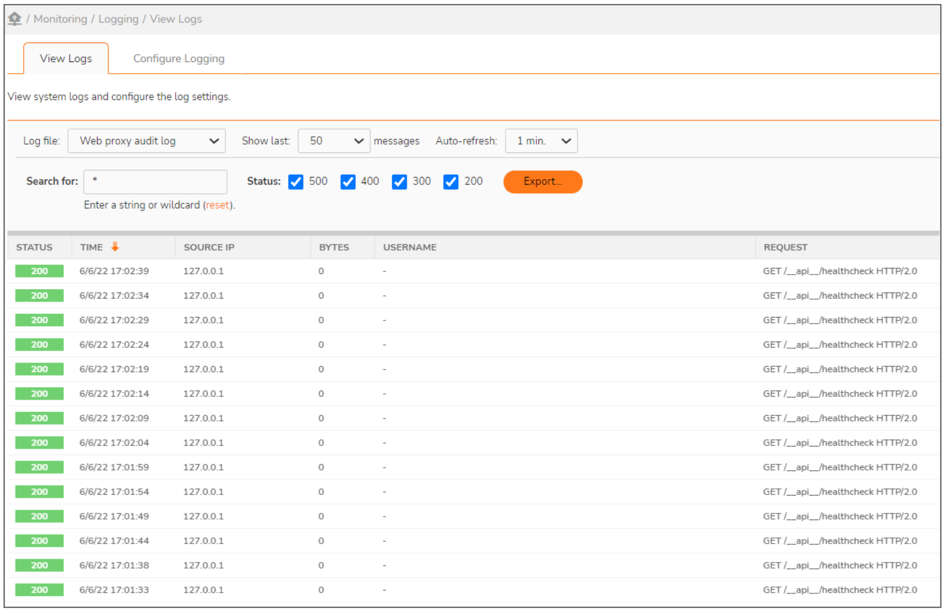
The Web proxy audit log provides detailed information about connection activity for users who are accessing resources using Web Proxy Access or Translated Access, including a list of users and the amount of data transferred.

To view the Web Proxy Audit log:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.

2. Select **Web proxy audit log** from the **Log file** drop-down menu.



View system logs and configure the log settings.

Log file: Web proxy audit log Show last: 50 messages Auto-refresh: 1 min.

Search for: * Status: ☑ 500 ☑ 400 ☑ 300 ☑ 200

Enter a string or wildcard (reset).

STATUS	TIME	SOURCE IP	BYTES	USERNAME	REQUEST
200	6/6/22 17:02:39	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:34	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:29	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:24	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:19	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:14	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:09	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:02:04	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:59	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:54	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:49	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:44	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:38	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0
200	6/6/22 17:01:33	127.0.0.1	0	-	GET /__api__/healthcheck HTTP/2.0

The **View Logs** page displays the information shown in the below table about the Web proxy audit log file.

Web Proxy Audit Log Information

Column	Description

Status	Displays color-coded return codes for each HTTP request. Move the pointer over an HTTP return code number to see explanatory text. The code numbers are in the following ranges and colors: • 500: server error (red) • 400: client error (orange) • 300: redirection (green) • 200: success (green)
Time	The date and time at which the request was received by the appliance.
Source IP	The IP address and port number of the computer that used the Web proxy service.
Bytes	The number of bytes sent in the body of the response, excluding the size of the HTTP headers.
Username	The name with which the user authenticated to the Web proxy service. You can search all log messages related to a specific user by clicking a username link.
Request	Shows the first line of the HTTP request, which contains the HTTP command (such as GET or POST), the requested resource, and the HTTP version number

ⓘ **NOTE:** For information on manually reviewing log files from the command-line interface on the appliance, see Web Proxy Audit Log.

Client Installation Logs (Windows)

When users log in to a realm, the access methods available to them depend on a few different things:

- The network access agents or clients that are permitted for a particular community, which is something that you specify when you set up a realm
- The user's environment: the operating system, browser, the availability of ActiveX or Java, and whether any clients or agents are already present

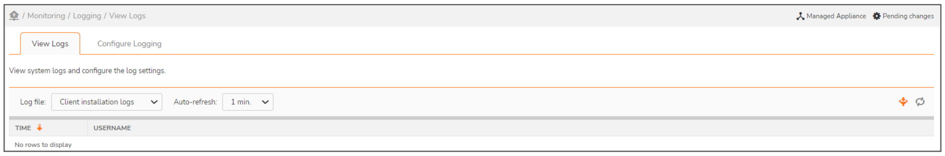
If something goes wrong during client or agent installation on a computer running Windows, the error is recorded in a client installation log. These logs are automatically uploaded to the appliance and listed in AMC if the user has Secure Endpoint Manager installed. See Client and Agent Provisioning (Windows) for details about Secure Endpoint Manager.

To view the list of client logs for all users:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.

2. Select **Client installation logs** from the **Log file** drop-down menu.



View system logs and configure the log settings.

Log file: Client installation logs   Auto-refresh: 1 min.

TIME	USERNAME
No rows to display	

You can sort the client installation logs by time or username; to download a log file, click on it. The log appends information about each step in the provisioning process: bootstrapping, provisioning new components, and interrogating the device (for device profile matching). The last set of information is probably where the installation problem occurred.

When troubleshooting, first look at a user's client installation log in AMC, and then (if necessary) the log file, `epiBootstrapper.log`, stored on the user's local machine in the `\Documents and Settings\<username>\Application Data\SMA1000\LogFiles` folder.

Configuring the logging settings for managed appliances

From 12.4.2 onwards, you can:

- View and change the log levels for all services on any number of appliances in the cluster.
- Send syslog data to the same SIEM platform.

To configure the logging settings for managed appliances:

ⓘ **NOTE:** Ensure, In CMS under **Central Management** > **Authentication Servers**, **Appliances share the same authentication servers** is selected.

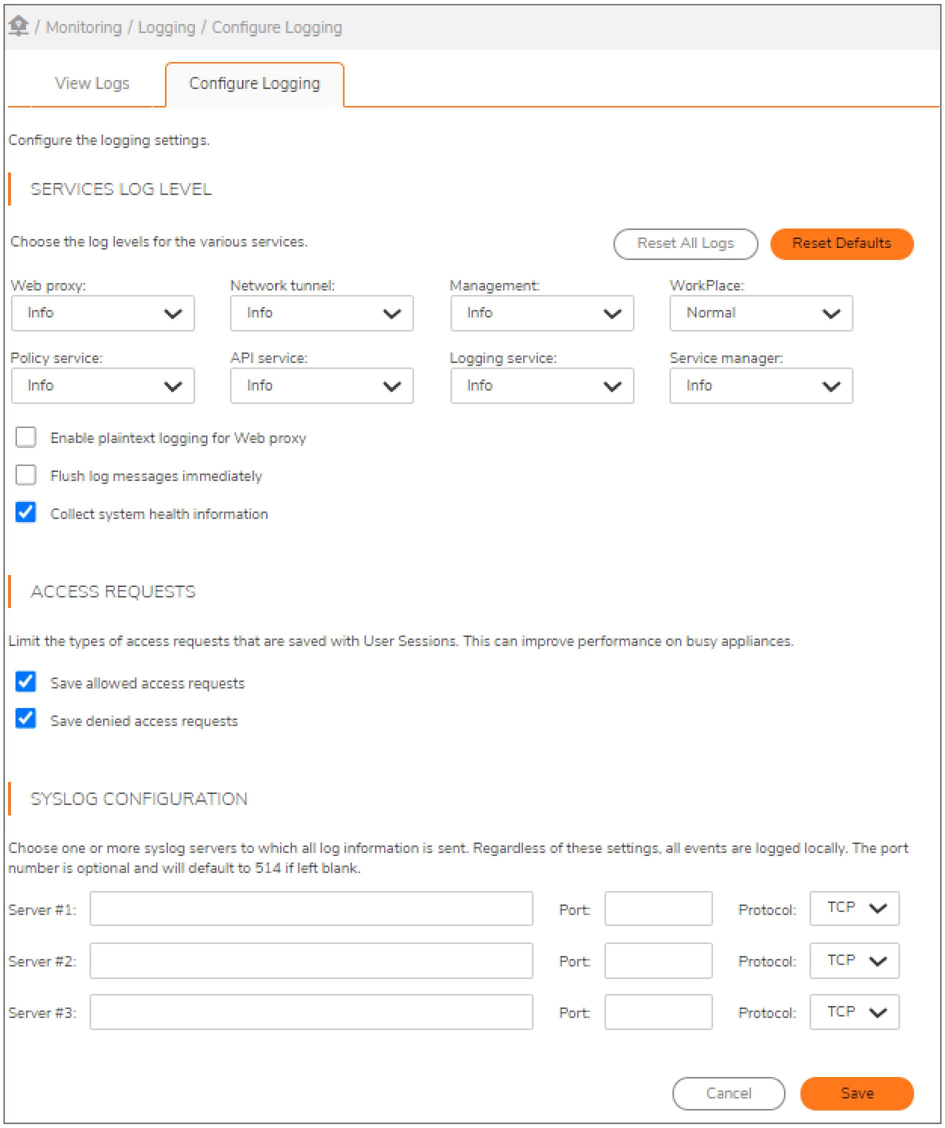
1. In the AMC, navigate to **Monitoring** > **Logging**.
2. Select the **Managed Appliance** tab.
3. Click on **All appliances** to adjust logging levels for all appliances or click on specific appliance.
   - Select **Enable plaintext logging for Web proxy**
     or
     Select **Flush log messages immediately**
     or
     Select **Collect system health information**
4. Click **OK**.

Setting Log Levels

You can specify how much detail is written to the message logs for each service. Increasing the message log detail requires more disk space and has a greater impact on system performance.

To set the logging level:

1. In the AMC, navigate to **Monitoring > Logging**.
   The **View Logs** page displays.
2. Click the **Configure Logging** tab.



Configure the logging settings.

SERVICES LOG LEVEL

Choose the log levels for the various services.

Web proxy: Info

Network tunnel: Info

Management: Info

WorkPlace: Normal

Policy service: Info

API service: Info

Logging service: Info

Service manager: Info

□ Enable plaintext logging for Web proxy

□ Flush log messages immediately

☑ Collect system health information

ACCESS REQUESTS

Limit the types of access requests that are saved with User Sessions. This can improve performance on busy appliances.

☑ Save allowed access requests

☑ Save denied access requests

SYSLOG CONFIGURATION

Choose one or more syslog servers to which all log information is sent. Regardless of these settings, all events are logged locally. The port number is optional and will default to 514 if left blank.

Server #1: Port: Protocol: TCP

Server #2: Port: Protocol: TCP

Server #3: Port: Protocol: TCP

3. Select the appropriate level of message detail for the services on the appliance, which are listed in order of increasing detail. The highest detail log levels (**Verbose** and **Debug**) are valuable for troubleshooting purposes, but they require more disk space and can have a significant performance impact: they should not be used in normal operation.
4. You can also configure the appliance to send system logs to one or more syslog servers. Type the IP addresses and port numbers for the syslog servers in the **Syslog configuration** area. Port **514** is the standard syslog-ng port, but you can use another port as needed to match your server configuration. Regardless of whether you configure syslog, all system events are logged locally.
5. Click **Save** or click **Cancel**to discard any changes you've made.

Configuring Access Request Logging

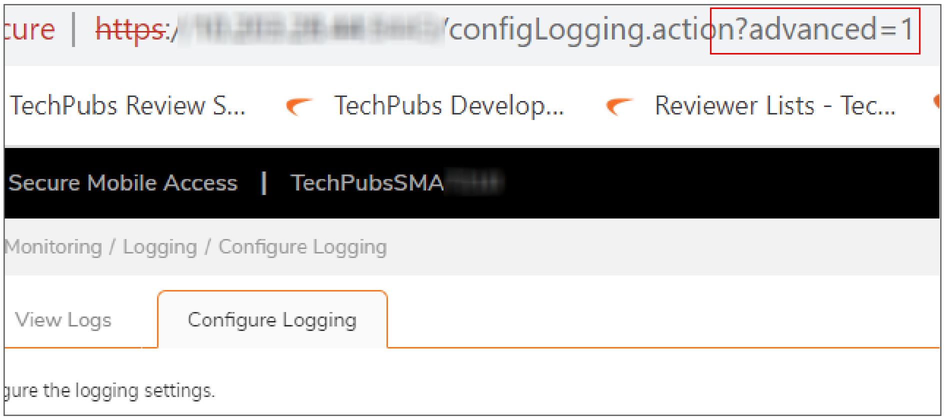
In SMA1000 12.4.3 you can limit the types of access requests that are saved with User Sessions.

Prerequisites:

- SMA/CMS running 12.4.3 firmware versions.

To configure access request overrides in AMC:

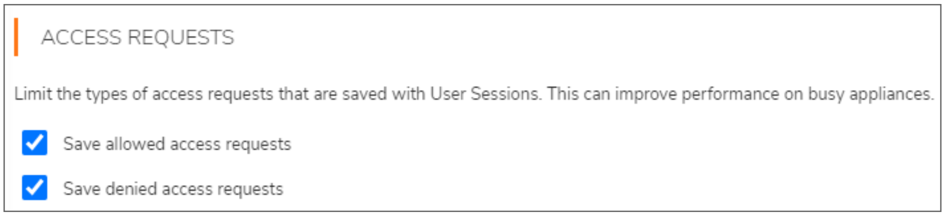
1. In the AMC, navigate to **Monitoring** > **Logging**.
2. Click **Configure Logging** tab.
3. Append **?advanced=1** in the URL.



ure | ~~https~~:/[redacted]/configLogging.action?advanced=1

ure the logging settings.

4. In the **Access Request** section select the following options to allow or deny the access request.



ACCESS REQUESTS

Limit the types of access requests that are saved with User Sessions. This can improve performance on busy appliances.

☑ Save allowed access requests

☑ Save denied access requests

Option	Description
Save allowed access requests	Log only allowed access requests
Save denied access requests	Log only denied access requests

5. Click **Save** to apply pending changes.

Sending messages to a syslog server

The SMA appliance can send system logs to a syslog server. Regardless of whether you configure syslog, all system events are logged locally. To avoid flooding the network with log information, the appliance forwards log messages for all the severity levels other than debug (emergency through informational).

For information on the syslog protocol, see RFC 3164 (http://www.ietf.org/rfc/rfc3164.txt).

To send log files to a syslog server:

1. In the AMC, navigate to **Monitoring > Logging**.

   The **View Logs** page displays.
2. Click the **Configure Logging** tab.
3. Under **Syslog configuration**, type the IP address and port numbers for one or more syslog servers. The default for the syslog-ng port is **514**, but you can use another port as needed to match your server configuration. Use the **Protocol** list to specify whether the appliance will communicate with syslog using the TCP or UDP or TLS protocol.
4. Click **Cancel** to discard any changes you've made, or click **Save**.

ⓘ **NOTE:** Because syslog data is not encrypted, sending log messages to an external server is a potential security issue.

Splunk Integration

The Secure Mobile Access 1000 appliance records system and user events in a series of log files. The Secure Mobile Access 1000 logs are very rich and complex, and it is difficult for customers to use in the context of Splunk and other enterprise reporting tools. To search and access the user events log files easier, SonicWallSMA1000 Splunk Add-on is integrated in the Splunk Server using the Splunk Common Information Model (CIM).

The SonicWallSMA1000 Splunk Add-on uses the following collection methods to collect the logs:

- Logs collected via syslog are:
  - Authentication
  - Change
  - Network sessions
  - Network Traffic
- Logs collected via API polling is:
  - Performance

Prerequisites:

- SMA/CMS running 12.4.2 firmware version or higher.
- Splunk Server 8.x and above.

Topics:

- Sending log files to Splunk server
- Installing Sonicwall SMA1000 Technical Add-on for Splunk
- Setting up new polling input in Splunk server
- Configuring syslog data input in Splunk server
- Searching the logs
- Reports provided in search

Sending log files to Splunk server

To send log files to a syslog server:

1. In the AMC, navigate to **Monitoring** > **Logging**.

   The **View Logs** page displays.

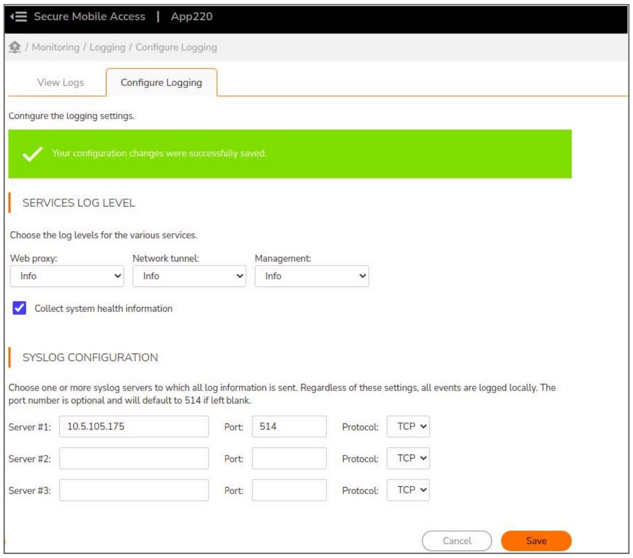
2. Click the **Configure Logging** tab.

3. Under **Syslog configuration**, type the following:

   a. Enter the splunk server IP in syslog server address.

   b. Enter the **Port** number defined in syslog server.

   c. Click **Save**.



Configure the logging settings.

Your configuration changes were successfully saved.

Choose the log levels for the various services.

Web proxy: Info

Network tunnel: Info

Management: Info

☑ Collect system health information

Choose one or more syslog servers to which all log information is sent. Regardless of these settings, all events are logged locally. The port number is optional and will default to 514 if left blank.

Server #1:	10.5.105.175	Port:	514	Protocol:	TCP
Server #2:		Port:		Protocol:	TCP
Server #3:		Port:		Protocol:	TCP

4. In the AMC, navigate to **User Access** > **Realms**.

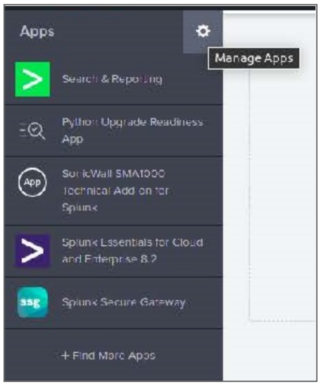
5. Click on the realm name.

6. Select the **Enable accounting records** checkbox to save accounting information about the selected realm.

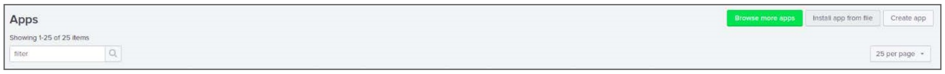
7. Click **Save**.

Installing Sonicwall SMA1000 Technical Add-on for Splunk

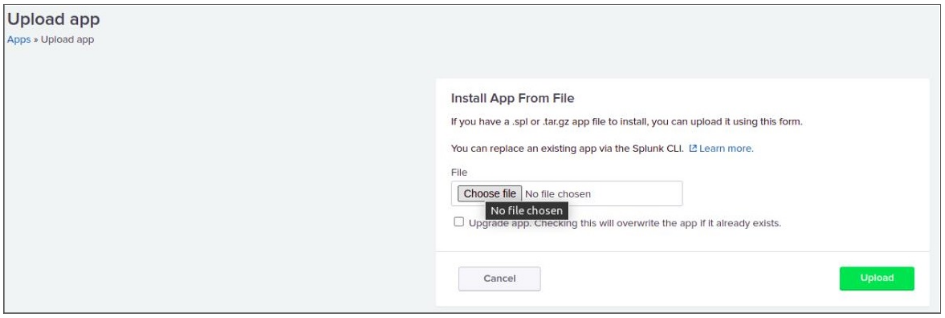
1. Login to the Splunk Server.
2. Click on settings icon to manage apps.


Apps
Manage Apps
Search & Reporting
Python Upgrade Readiness App
SonicWall SMA1000 Technical Add on for Splunk
Splunk Essentials for Cloud and Enterprise 8.2
Splunk Secure Gateway
+ Find More Apps

3. Click on **Install app from file**.



4. Click **Choose file** and select **sonicwall_sma1000_ta-1.0.x.tar.gz**.



If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File

☐ Upgrade app. Checking this will overwrite the app if it already exists.

5. Click **Upload**.

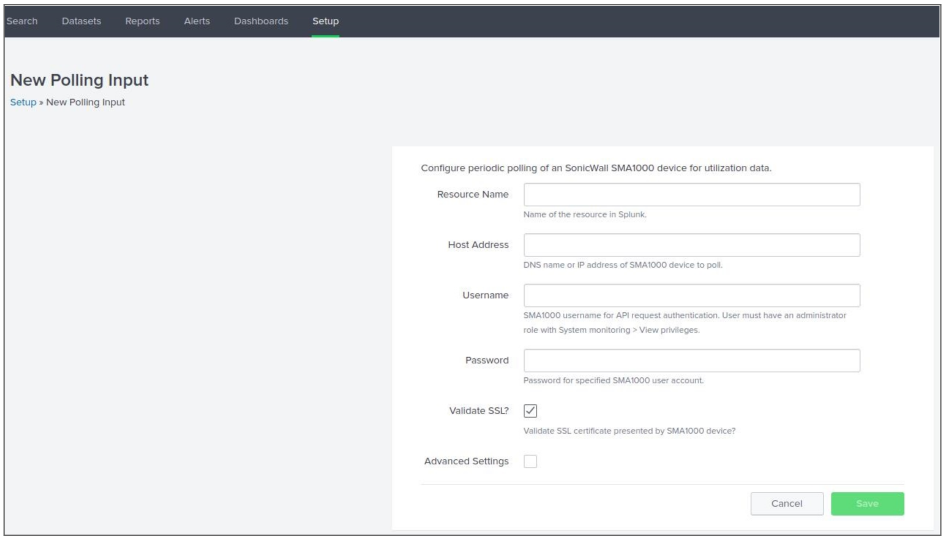
   ⓘ | **TIP:** You can enable the **Upgrade app** checkbox to upgrade the application if already exists.

6. In the **Apps** page, you can find **SonicWall SMA1000 Technical Add-on for Splunk** is added.
7. Click **Launch App**.

Setting up new polling input in Splunk server

To setup a new polling input in Splunk server:

1. Login to the Splunk Server.
2. Go to **Setup** tab and click **New**.



New Polling Input

Setup » New Polling Input

Configure periodic polling of an SonicWall SMA1000 device for utilization data.

Resource Name

Name of the resource in Splunk.

Host Address

DNS name or IP address of SMA1000 device to poll.

Username

SMA1000 username for API request authentication. User must have an administrator role with System monitoring > View privileges.

Password

Password for specified SMA1000 user account.

Validate SSL? ☑

Validate SSL certificate presented by SMA1000 device?

Advanced Settings □

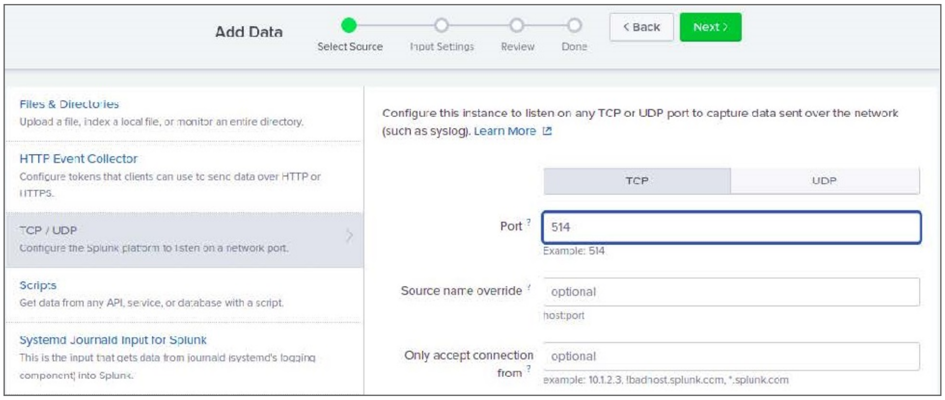
3. In the **Resource Name** field enter the name of the appliance.
4. In the **Host Address** field enter the appliance IP address.
5. In the **Username** field enter **local/admin**.
6. In the **Password** field enter the admin password.
7. Enable the **Validate SSL** checkbox and click **Save**.
8. Repeat the procedure to add more appliances.

Configuring syslog data input in Splunk server

To configure the syslog data input in Splunk server:

1. Login to Splunk server.
2. Navigate to **Settings** > **Data** > **Data inputs** > **TCP**.
3. Click **New Local TCP**.
4. In **Port** enter the port number.

   ⓘ | **TIP:** For example, you can enter 514.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

Port: 514
Example: 514

Source name override: optional
host:port

Only accept connection from: optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

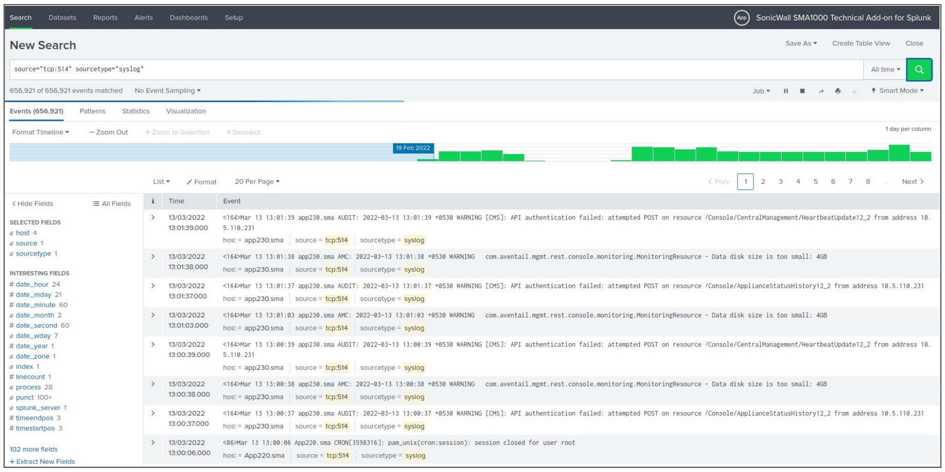
5. Click **Next**.
6. In **Select Source Type** select **syslog**.
7. Leave other fields as default and click on **Review**.
8. Click **Submit**.

Searching the logs

Ensure you have configured the port number in AMC and Splunk server.

1. Login to Splunk server.
2. Click **Search**.
3. Type a keyword (for example, type username to search log lines with the username or type * symbol) to search all syslogs.

   All the log files are displayed. You can view each event individually.



```
source="tcp:514" sourcetype="syslog"
```

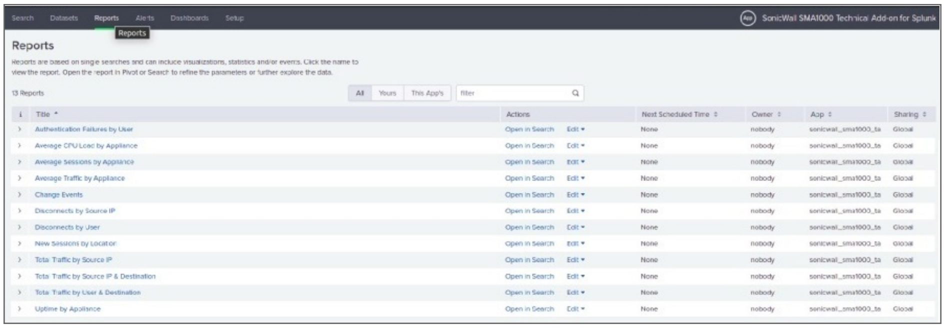
656,921 of 656,921 events matched

i	Time	Event
›	13/03/2022 13:01:39.000	<164>Mar 13 13:01:39 app230.sma AUDIT: 2022-03-13 13:01:39 +0530 WARNING [CMS]: API authentication failed: attempted POST on resource /Console/CentralManagement/HeartbeatUpdate12_2 from address 10.5.110.231 host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:01:38.000	<164>Mar 13 13:01:38 app230.sma AMC: 2022-03-13 13:01:38 +0530 WARNING com.aventail.mgmt.rest.console.monitoring.MonitoringResource - Data disk size is too small: 4GB host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:01:37.000	<164>Mar 13 13:01:37 app230.sma AUDIT: 2022-03-13 13:01:37 +0530 WARNING [CMS]: API authentication failed: attempted POST on resource /Console/ApplianceStatusHistory12_2 from address 10.5.110.231 host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:01:03.000	<164>Mar 13 13:01:03 app230.sma AMC: 2022-03-13 13:01:03 +0530 WARNING com.aventail.mgmt.rest.console.monitoring.MonitoringResource - Data disk size is too small: 4GB host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:00:39.000	<164>Mar 13 13:00:39 app230.sma AUDIT: 2022-03-13 13:00:39 +0530 WARNING [CMS]: API authentication failed: attempted POST on resource /Console/CentralManagement/HeartbeatUpdate12_2 from address 10.5.110.231 host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:00:38.000	<164>Mar 13 13:00:38 app230.sma AMC: 2022-03-13 13:00:38 +0530 WARNING com.aventail.mgmt.rest.console.monitoring.MonitoringResource - Data disk size is too small: 4GB host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:00:37.000	<164>Mar 13 13:00:37 app230.sma AUDIT: 2022-03-13 13:00:37 +0530 WARNING [CMS]: API authentication failed: attempted POST on resource /Console/ApplianceStatusHistory12_2 from address 10.5.110.231 host = app230.sma source = tcp:514 sourcetype = syslog
›	13/03/2022 13:00:06.000	<86>Mar 13 13:00:06 App220.sma CRON[3598316]: pam_unix(cron:session): session closed for user root host = App220.sma source = tcp:514 sourcetype = syslog

Reports provided in search

To view the reports:

1. Login to Splunk server.
2. Go to the **Reports** tab.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

13 Reports

i	Title	Actions		Next Scheduled Time	Owner	App	Sharing
›	Authentication Failures by User	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Average CPU Load by Appliance	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Average Sessions by Appliance	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Average Traffic by Appliance	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Change Events	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Disconnects by Source IP	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Disconnects by User	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	New Sessions by Location	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Total Traffic by Source IP	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Total Traffic by Source IP & Destination	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Total Traffic by User & Destination	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global
›	Uptime by Appliance	Open in Search	Edit ▾	None	nobody	sonicwall_sma1000_ta	Global

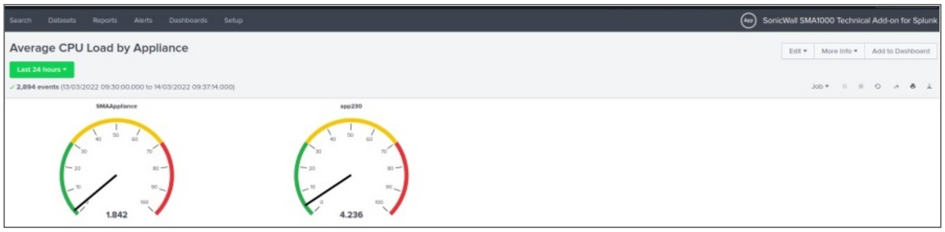
3. Click on any report **Title** to view the reports.

   Following files are displayed:

   - Average CPU Load by Appliance
   - Change Events
   - Disconnects by Source IP
   - Disconnects by User
   - New Sessions by Location
   - Total Traffic by Source IP
   - Total Traffic by Source IP & Destination
   - Total Traffic by User & Destination
   - Uptime by Host
   - Authentication Failures by User
   - Average Sessions by Appliance
   - Average Traffic by Appliance

   For example:

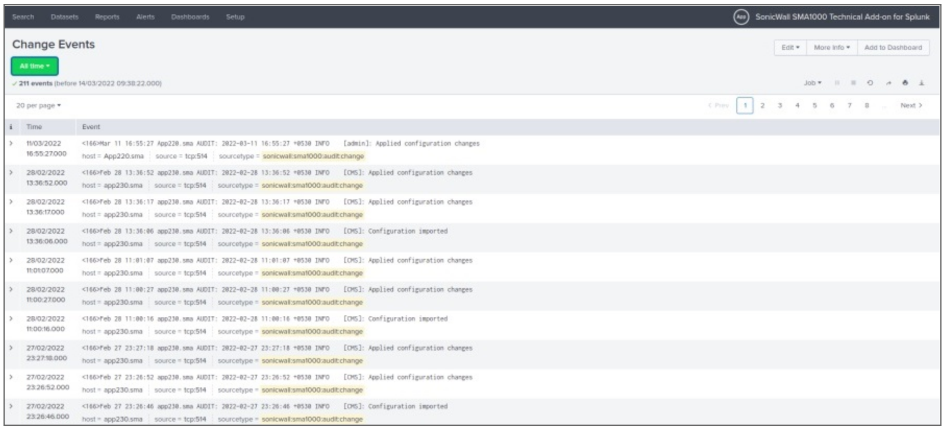
   - If you click on Average CPU Load by Appliance displays the average CPU load for all appliances added in Splunk Server.



Average CPU Load by Appliance

✓ 2,894 events (13/03/2022 09:30:00.000 to 14/03/2022 09:37:14.000)

- If you click on Change events, it displays the reports of AMC Configuration changes made in added appliances.



Change Events

✓ 211 events (before 14/03/2022 09:38:22.000)

i	Time	Event
>	11/03/2022 16:55:27.000	<166>Mar 11 16:55:27 App220.sma AUDIT: 2022-03-11 16:55:27 +0530 INFO [admin]: Applied configuration changes host = App220.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 13:36:52.000	<166>Feb 28 13:36:52 app230.sma AUDIT: 2022-02-28 13:36:52 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 13:36:17.000	<166>Feb 28 13:36:17 app230.sma AUDIT: 2022-02-28 13:36:17 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 13:36:06.000	<166>Feb 28 13:36:06 app230.sma AUDIT: 2022-02-28 13:36:06 +0530 INFO [CMS]: Configuration imported host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 11:01:07.000	<166>Feb 28 11:01:07 app230.sma AUDIT: 2022-02-28 11:01:07 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 11:00:27.000	<166>Feb 28 11:00:27 app230.sma AUDIT: 2022-02-28 11:00:27 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	28/02/2022 11:00:16.000	<166>Feb 28 11:00:16 app230.sma AUDIT: 2022-02-28 11:00:16 +0530 INFO [CMS]: Configuration imported host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	27/02/2022 23:27:18.000	<166>Feb 27 23:27:18 app230.sma AUDIT: 2022-02-27 23:27:18 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	27/02/2022 23:26:52.000	<166>Feb 27 23:26:52 app230.sma AUDIT: 2022-02-27 23:26:52 +0530 INFO [CMS]: Applied configuration changes host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change
>	27/02/2022 23:26:46.000	<166>Feb 27 23:26:46 app230.sma AUDIT: 2022-02-27 23:26:46 +0530 INFO [CMS]: Configuration imported host = app230.sma source = tcp:514 sourcetype = sonicwall:sma1000:audit:change

ⓘ | **NOTE:** Important notes on Reports.

- For monitoring user sessions reports, for instance **New Sessions by Location** make sure "**Accounting Records** is enabled in the Realm in AMC.
- **New Sessions by Location** reports uses IP geolocation, so users connecting from private IPs will not be shown in report. To test this report you would need to create session(s) to the appliance that originate from public IPs.

Monitoring the Appliance

AMC displays a variety of information that is helpful in monitoring basic system settings, disk and memory usage, current connections, and network bandwidth use.

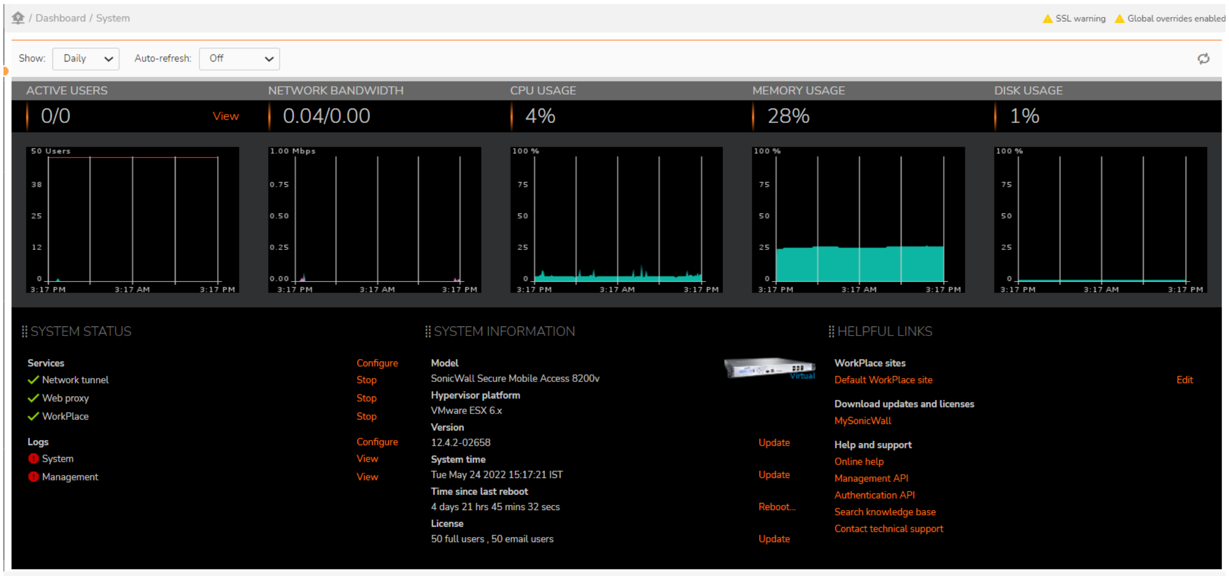
This section describes how to monitor system status and active users, and how to terminate VPN connections for selected users.

Topics:

Monitoring Overall Activity

The **AMC Dashboard** displays a graphical summary of information that is helpful in monitoring system status. The graphs show average usage for the selected interval and is optionally refreshed at intervals based on your Auto-refresh selection.

ⓘ **NOTE:** Warnings are displayed based on the selected interval. Change the interval to increase or decrease warnings.



/ Dashboard / System

SSL warning Global overrides enabled

Show: Daily Auto-refresh: Off

ACTIVE USERS 0/0 View

NETWORK BANDWIDTH 0.04/0.00

CPU USAGE 4%

MEMORY USAGE 28%

DISK USAGE 1%

SYSTEM STATUS

Services — Configure
✓ Network tunnel — Stop
✓ Web proxy — Stop
✓ WorkPlace — Stop

Logs — Configure
System — View
Management — View

SYSTEM INFORMATION

Model
SonicWall Secure Mobile Access 8200v

Hypervisor platform
VMware ESX 6.x

Version
12.4.2-02658 — Update

System time
Tue May 24 2022 15:17:21 IST — Update

Time since last reboot
4 days 21 hrs 45 mins 32 secs — Reboot...

License
50 full users , 50 email users — Update

HELPFUL LINKS

WorkPlace sites
Default WorkPlace site — Edit

Download updates and licenses
MySonicWall

Help and support
Online help
Management API
Authentication API
Search knowledge base
Contact technical support

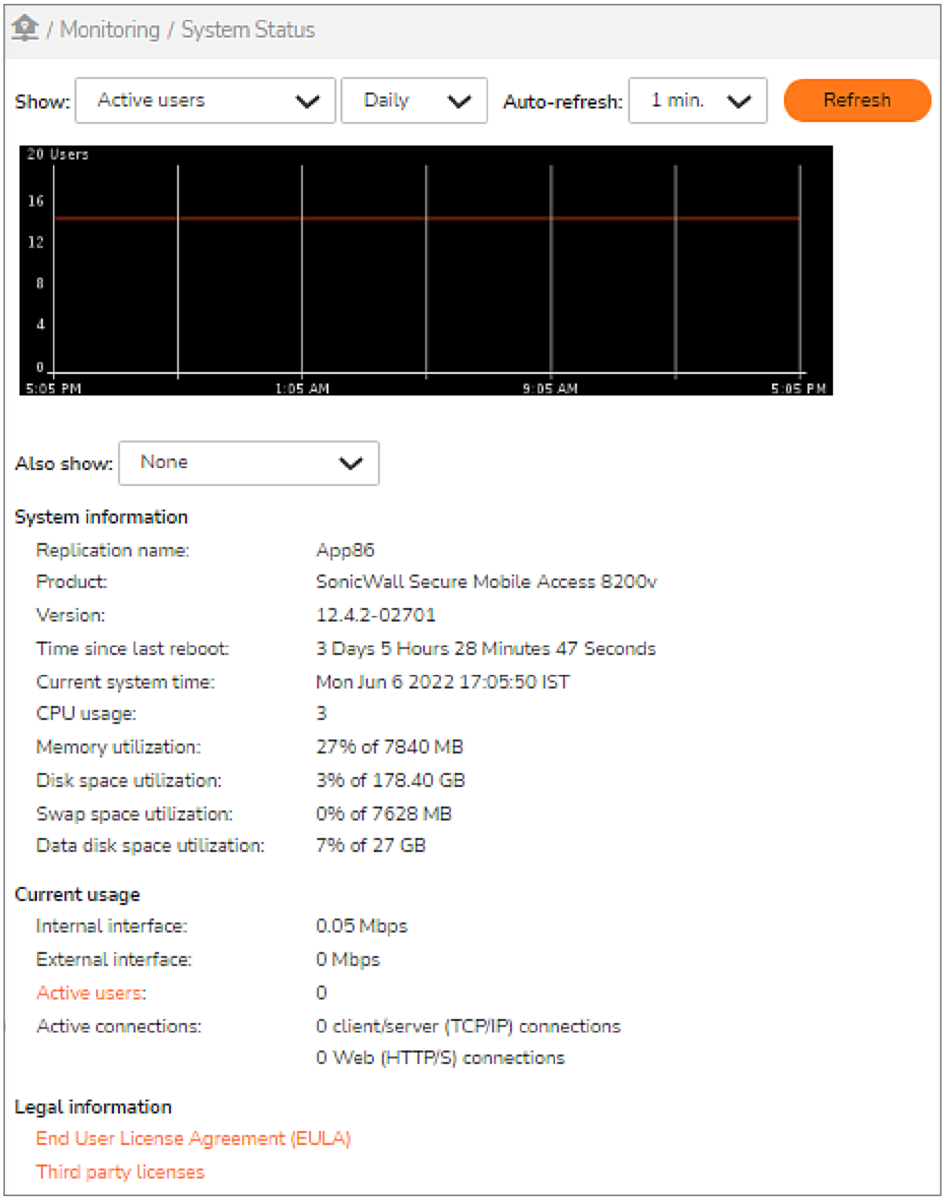
Click the **Home** link at the top right of an AMC page to display the AMC home page. In addition to the system status graphs, this page provides a convenient access point to:

- Often used functions, such as starting and stopping services and viewing logs.
- Hardware and licensing information.
- Links to the default WorkPlace, MySonicWall.com, online help, and support options.

Monitoring System Status

1. In the AMC, navigate to **Monitoring > System Status**.

   The **System Status page** displays, displaying information about the appliance's current status, such as memory utilization.



System information

Replication name:	App86
Product:	SonicWall Secure Mobile Access 8200v
Version:	12.4.2-02701
Time since last reboot:	3 Days 5 Hours 28 Minutes 47 Seconds
Current system time:	Mon Jun 6 2022 17:05:50 IST
CPU usage:	3
Memory utilization:	27% of 7840 MB
Disk space utilization:	3% of 178.40 GB
Swap space utilization:	0% of 7628 MB
Data disk space utilization:	7% of 27 GB

Current usage

Internal interface:	0.05 Mbps
External interface:	0 Mbps
Active users:	0
Active connections:	0 client/server (TCP/IP) connections 0 Web (HTTP/S) connections

Legal information

End User License Agreement (EULA)

Third party licenses

2. In the **Show** drop-down menu, select the type of data you want to view; see the System status data table.

System Status Data

Type of data	Description

Active users (default)	Displays the number of active user sessions for the specified time period. This graph includes a horizontal line that indicates the maximum number of concurrent users allowed by your license. ⓘ **NOTE:** Active user sessions are not the same as licensed ones; for more information, see Open vs Licensed Sessions.
CPU utilization	Displays the percentage of the CPU capacity that was used for the specified time period.
Memory utilization	Displays the percentage of memory that was used for the specified time period. The percentage is calculated from information returned by the `meminfo` utility on the appliance: `((MemTotal - Cached - MemFree) / MemTotal) * 100`
Network bandwidth	Displays the network bandwidth in Mbps for the specified time period. If both the internal and external interfaces are enabled, graph data for the internal interface is represented by a green line and data for the external interface is displayed in blue. The scale of this graph automatically adjusts to reflect the amount of traffic (for example, the graph might use a 1 Mbps scale or a 100 Mbps scale, depending on traffic).
Swap utilization	Displays the amount of free swap space available for the specified time period.
Disk space utilization	Displays the percentage of disk space used for the specified time period.

3. In the second **Show** drop-down menu, indicate the time interval you want to show; see the below table.

   Time Interval Selection

Interval	Description
Hourly	Displays average activity during the last hour based on samples collected every 20 seconds.
Daily	Displays average activity for the last day based on samples collected every ten minutes.
Weekly	Displays average activity for the last week based on samples collected every 60 minutes.
Monthly	Displays average activity for the last 32 days based on samples collected every four hours (six samples per day).

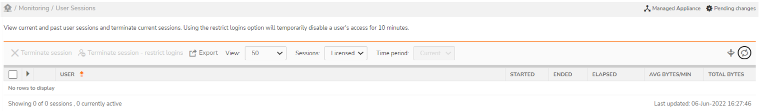
4. In the **Auto-refresh** drop-down menu, select a value that indicates how often AMC will automatically update the selected data.
5. Optionally, in the **Also show** drop-down menu, you can select another type of data graph. This can be useful if you want to compare two types of data for a given time period. The default is **None**.
6. To update the page at any time, click **Refresh**.

Viewing User Sessions

You can monitor, troubleshoot or terminate user sessions on your appliance. By sorting through the list and filtering the sessions—by user name, realm (authentication server), community, access agent, traffic load, and so on—you can narrow your search to particular sessions and view further details about them. Here are two filtering examples.

To view all open user sessions:

1. In the AMC, navigate to **Monitoring > User Sessions**.

   View current and past user sessions and terminate current sessions. Using the restrict logins option will temporarily disable a user's access for 10 minutes.

   View: 50 Sessions: Licensed Time period: Current

   No rows to display

   Showing 0 of 0 sessions , 0 currently active

   Last updated: 06-Jun-2022 16:27:46

   You can get a quick read on what state a session is in by looking at its icon. See Open vs Licensed Sessions for a complete description of each state.

2. In the **View** list, select **All open** sessions. This displays sessions that are either licensed or idle. An idle session is one that can be resumed: its license is released after the connection is inactive for more than15 minutes, but up until that moment the session can be resumed. See Open vs Licensed Sessions for more information on what sessions are considered open.

3. You can filter your list of sessions further using a combination of other properties, such as realm and zone. Click **Refresh** to update the list of sessions based on your filters.

4. Review the session list. To resort the list, click the heading at the top of a column.

5. For a quick summary of a particular session, expand the item in the session list.

   For complete session details, such as the resource a user attempted to access and what policy rules were applied in the process, click the username link. See Viewing User Access and Policy Details for more information on this troubleshooting tool.

To search for sessions with a high traffic load:

1. In the AMC, navigate to **Monitoring > User Sessions**.

2. In the **View** list, select **All** sessions.

3. If you plan to end sessions that are taking up too much bandwidth, restrict the list to licensed sessions: in the **Filters** area, select **Licensed** in the **Status** list, and then click **Refresh**.

4. To isolate the time range you’re interested in, make a selection in the **Time period** drop-down menu. Select:

   - **All** to see data from sessions that are up to one week old.
   - **Last 24 hours** to see user activity for the last day.
   - **Custom** to specify a particular range by date and time.

5. Click **Refresh** to view updated results.

6. To find out which sessions involve the most traffic, sort the list by clicking **Avg byte/Min** (the amount of traffic for the last hour) or **Total byte** (the total amount for the session) at the top of the column.

Open vs Licensed Sessions

When you look at user sessions in AMC it’s important to understand the distinction between different types of sessions. For example, if a user has a question about access to a resource, you will want to see all sessions associated with that user (even the failed ones), not just the ones that are licensed. Session types are defined as:

- Licensed Sessions
- All Open Sessions
- Authorization Terms Not Accepted
- All Sessions

Licensed Sessions

A licensed session does not represent a person, but rather a user authentication. A user who is logged in on two devices, for example, consumes two licenses as soon as a resource protected by the appliance is accessed.

Until the user explicitly logs out of a session or the session has timed out (after 15 minutes of inactivity), a license is consumed (simply closing the browser window in WorkPlace, for example, does not free up a license).

All Open Sessions

An open session is defined as a session that is either licensed or that can be resumed. This idle, can-be-resumed, state is different for browser and tunnel sessions:

- A browser session will have its license released after the connection is inactive for more than 15 minutes.
- A Connect Tunnel session will have its license released 15 minutes after the tunnel has been disconnected due to a network event, for example, when a mobile user moves out of range or a laptop lid is closed. (Even when the user has stopped using a tunnel session, it remains active because of network traffic, such as keep-alive packets).

Unlicensed sessions in this open state can be resumed as long as the authentication token remains valid and a license is available when the session is resumed. By default, the authentication token is valid several hours after a session is started.

Authorization Terms Not Accepted

This category is used for sessions that were blocked because the user was using a personal device and did not accept the authorization terms.

All Sessions

This category includes all open sessions, plus sessions that were ended or where the login has failed after successive retries. If the user abandons his or her login attempts before receiving a final failure message, no information about those attempts is displayed in this list. Data about sessions that ended more than 7 days ago is discarded.

ⓘ | **NOTE:** See How Licenses Are Calculated for more information.

Ending User Sessions

You can immediately terminate a user’s session, even if the user has multiple connections on different services or nodes, or temporarily disable a user’s network access for 10 minutes (the user can log in to the network again after that period if your access policy allows it). To permanently prevent a user from logging in to your VPN, you must do one of the following:

- Modify the applicable access control rules
- Modify or delete the applicable user and group definitions
- Delete the user from your user directory

To end open user sessions:

1. In the AMC, navigate to **Monitoring > User Sessions**.
2. In the **View** lists, select the number of sessions you want to display, and then select **All open** (only sessions that are open can be terminated).
3. You can filter the list of sessions using a combination of other properties:
    - **User**: Enter all or part of a user name. You can use wildcard characters (`*` or `?`) anywhere in the search string.
    - **Realm**: Select a realm, or all realms.
    - **Community**: Select a community, or all communities. If you selected a realm, the communities you see in this list are restricted to those that are associated with it.
    - **Zone**: Select a zone, or all zones.
    - **Agent**: Select an agent or All access agents, or specify that none have been activated (translation only).
    - **Platform**: Select a platform or All platforms.
    - **Login Status**: Select a login status, or all status.
    - **Version**: Select a version, or all versions.
    - **License Type**: Select a license type, or all license types
4. There are two ways to terminate sessions manually in AMC. Only open sessions—those for which there is either a license or those that can be resumed—can be terminated. Select the checkbox next to any session you want to end, or select the checkbox at the top to select all the users in the list, and then click one of the session termination buttons:
    - **Terminate session** – When you click **Terminate session**, all connections associated with the selected sessions are terminated. This is a good way to free up a license from an idle session, for example. Termination occurs on a session-by-session basis, so if a user has several sessions you can be selective about which ones you end. The user whose session was terminated can immediately reauthenticate and log in to the appliance.
    - **Terminate session - restrict logins** – This type of termination is the same as above, but there is a ten-minute interval during which the user is not allowed to generate new sessions. If there are any existing sessions, they can be used, but until ten minutes elapse, no new sessions can be created.

This is the type of termination you would use, for example, if you wanted to end all of a user's sessions and prevent any new ones from being established while you remove his or her credentials from the authentication store.

Viewing User Access and Policy Details

If a user is experiencing trouble with a session—for example, he is logged in but cannot establish a connection or is denied access to resources—you can use the **Session Details** page to diagnose the problem. It enables you to troubleshoot a session, whether or not it's still active, by assessing its status, determining why a user's device is classified into a particular zone, and discovering what policy rules are applied, editing them as needed.

To view user session details:

1. In the AMC, navigate to **Monitoring > User Sessions**.
2. 2 Click the username link for the session you want more details about; if needed, narrow the displayed list by setting filters, and then click **Refresh**.
    - To troubleshoot access to resources, look at the **Access requests** list. You can expand a list item to see the access control rule that determined whether this particular connection request should be allowed or denied. If the rule still exists, you'll also see a link for editing the item.
    - Information for resources accessed using application access control identify the client software and platform for the session, the application used to access the resource, and the rule that allowed or denied access.
    - An End Point Control zone classifies a connection request based on the presence or absence of a device profile. On the **Zone classification** page you can see what EPC zones (if any) were evaluated during this session and what the outcome of each evaluation was. In this example, the mobile device was placed in the *Pocket PC* zone, but it did not match the *Equipment ID* device profile.
    - If the user's session has any current Connect Tunnel connections, they are listed by IP address on the **Active connections** page. Other access agents are not listed here because they do not keep the VPN connection open.
    - If the user connected using a personal device, device and authorization information is provided on the **Device Authorization** page. Users who were denied access because they did not accept the authorization terms are also identified on this page.
    - If the user connected using application access control, information about the applications found on the end point that are under control are also identified.

Exporting User Session Data

User session data can be exported from AMC to a comma-separated (`csv`) file that can be displayed and edited in Microsoft Excel. Once user session data is exported to a `csv` file, you may archive user session data indefinitely, create custom reports without using Secure Mobile Access Advanced Reporting (AAR), or use the file for any other special needs.

To export user session data to a CSV file:

1. In the AMC, navigate to **Monitoring > User Sessions**.
2. Optionally, filter the displayed user data so that only the data you want to export is displayed. See Viewing User Sessions for additional filtering information.
3. Click the **Export** button located at the top of the user session data.

   ⓘ **NOTE:** The Export button is enabled only if the Administrator has view access to the **User Sessions** page.
4. When the File Download page displays, click the **Save** button.
5. Select the location on the local computer and file name where user data should be saved or use the defaults. The default file name is UserSessions.csv and default location is your `Downloads` folder.
6. Click the **Save** button to export user session data to the csv file. All user sessions that meet the current filter criteria are exported.

The `csv` file may include the information shown in the below table for each user session, depending on the filters used.

User Session Data

Type of data	**Description**
System Version	Secure Mobile Access version number
Session ID	Unique numeric ID used to identify the session internally
State	State of user session: **Login Failed**, **Licensed**, **Idle**, or **Ended**
Username	Short username
Long Username	Full username and realm, including Common Name (CN) for AD/LDAP sessions
Start Time	Session start time in MM/DD/YYYY HH:MM:SS format, uses appliance local time
End Time	Session end time in MM/DD/YYYY HH:MM:SS format or blank if session is Idle or Licensed
Elapsed Seconds	Seconds between the session start and end times or start and current time for active and idle sessions
Average Bytes per Minute (Last Hour)	Average bytes (upload and download) per minute used by session over the last hour, used to determine high-usage users/sessions
Total bytes	Total number of bytes uploaded and downloaded by session
Realm	Realm name used to authenticate the user
Community	Community name the user was placed in
Zone	Zone the user/device was placed in
Access Agents	Access Agents used: Web only, Tunnel, Tunnel (ESP), OnDemand, Web Proxy, or Exchange
Agent Version	Connect Agent version number
Platform Version	Client platform version number

Remote Address	IP address of the client computer
Local Address	Local address assigned to the client connection, left blank for non-tunnel sessions

Following is an example of a user session `csv` file generated by AMC:

Version,SessionID,State,Username,LongUsername,StartTime,EndTime,ElapsedSeconds,AverageBytesPerMinuteLastHour,TotalBytes,Realm,Community,Zone,EPCAgent,AccessAgents,AgentVersion,PlatformVersionRemoteAdd ress,LocalAddress

```
12.4.1-02327,2,3,Licensed,"admin(admin)@(local)",5/10/2019
14:35,,157,5226,13503,local,"Default community","Default zone",,"Connect
Tunnel",12.20.267,"10.0.17763 Build 17763" ,192.168.212.1,2.0.0.2
```

SNMP Configuration

If you have an SNMP (Simple Network Management Protocol) tool, you can use it to monitor the appliance as an SNMP agent. The appliance supports SNMP versions 2 and 3, and provides a variety of management data in Management Information Base (MIB) II format.

You can enable SNMPv2 or SNMPv3, but not both at the same time. When SNMPv2 is enabled, SNMPv3 requests are ignored. When SNMPv3 is enabled, SNMPv2 requests are ignored. You can also disable SNMP support entirely, in which case any SNMP request directed at the system will be ignored and no traps will be generated.

SNMPv3 addresses the security deficiencies that have plagued both SNMPv1 and SNMPv2. SNMPv3 supports all the operations defined by versions 1 and 2. The new security functionality provided by SNMPv3 can be generally divided into three principle areas: authentication, privacy (encryption), and access control.

ⓘ | **NOTE:** SNMPv3 is the recommended selection for the best security.

Where authentication in SNMPv2 was provided, insecurely, by the clear text community string, authentication in SNMPv3 uses the SHA algorithm to provide secure authentication. For each SNMP user, both a username and a passcode as well as the desired algorithm are configured on the agent (in our case, the SMA appliance) and must match the username, passcode, and algorithm choice provided to the management software that will be communicating with the appliance.

Prior to SNMPv3, all communications were unencrypted. In SNMPv3, the AES algorithm is used to encrypt and decrypt SNMP messages. As with authentication, a username, password and encryption algorithm are used to seed the encryption and must be configured on both the agent and the management station.

The combined authentication and encryption levels supported by Secure Mobile Access for SNMPv3 are shown in the below table.

Combined Authentication And Encryption Levels

Level	Authentication	Encryption	Effect
noAuthNoPriv	Username	No	Uses a username match for authentication.

authNoPriv	SHA	No	Provides authentication based on the HMAC-SHA algorithm.
authPriv	SHA	AES	Provides authentication based on the HMAC-SHA algorithm. Provides AES encryption in addition to authentication.

Topics:

- Configuring SNMP
- Downloading the MIB File
- Retrieving Management Data Using SNMP
- MIB Data

Configuring SNMP

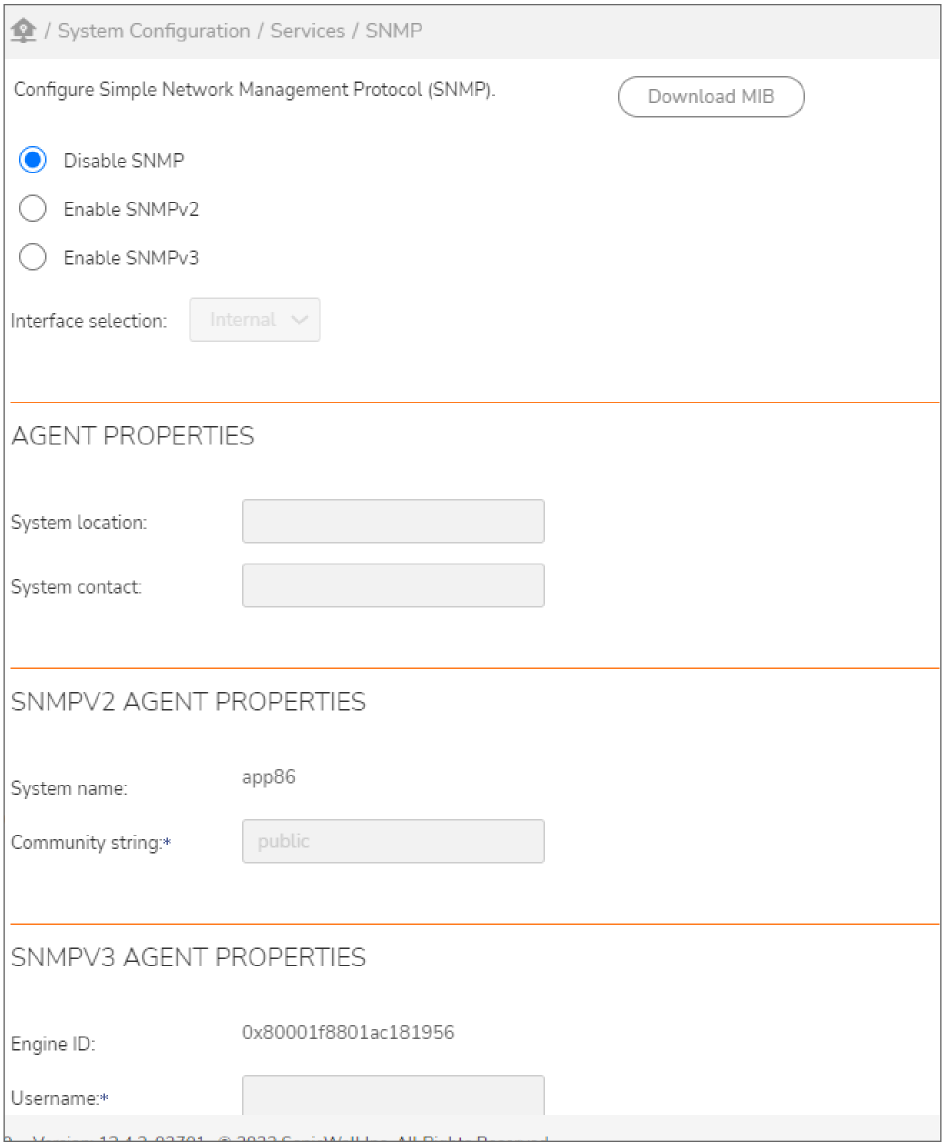
This section describes how to configure SNMP settings in AMC.

ⓘ | **NOTE:**

- You must configure your SNMP manager with the Management Information Base (MIB) used by the appliance. The appliance supports version 4.2.3 of the University of California, Davis (UCD) MIB, and MIB II. For SNMPv2, you must also configure your SNMP manager with the community string required to query the appliance. For SNMPv3, configure your SNMP manager with the same username, passcode, and algorithm choice as configured on the appliance.
- Ensure that your internal firewalls are configured to allow port 161/udp traffic.

To configure SNMP:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Network services** section, click the **Configure** link under **SNMP**.



/ System Configuration / Services / SNMP

Configure Simple Network Management Protocol (SNMP).

● Disable SNMP

○ Enable SNMPv2

○ Enable SNMPv3

Interface selection: Internal

AGENT PROPERTIES

System location:

System contact:

SNMPV2 AGENT PROPERTIES

System name: app86

Community string:* public

SNMPV3 AGENT PROPERTIES

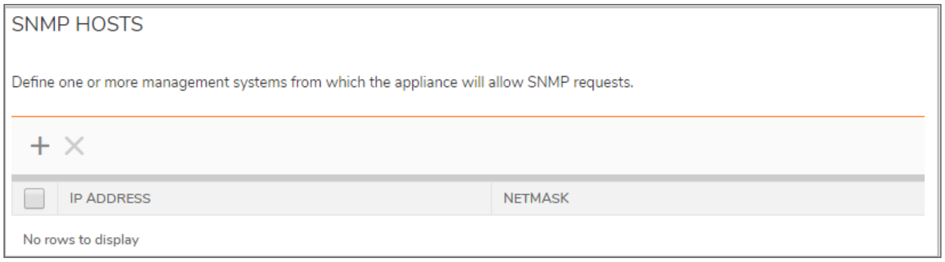
Engine ID: 0x80001f8801ac181956

Username:*

3. To enable SNMP, select either the **Enable SNMPv2** or the **Enable SNMPv3** radio button. (If you leave this page to configure SNMP hosts before clicking **Save**, the status of this setting will not be saved.) To disable SNMP, select the **Disable SNMP** radio button and then click **Save**.
4. Select the network interface you want SNMP to use by selecting the appropriate option (**Internal**, **External**, or **Both**) from the **Interface selection** drop-down menu.
5. Under **Agent properties**, describe the appliance agent in the **System location** and **System contact** fields. For example, you might specify the physical location of the appliance (for example, *Server lab*) and the system administrator contact information (such as *Jim Jamerson, 206-555-1212*).
6. If using SNMPv2, under **SNMPv2 Agent properties**, type the string your network management tool uses to query the SMA appliance in the **Community string** field. This field is required, and set to **public** by default. It is a good security practice to change your community string to a different passphrase because

public is not secure.

7. If using SNMPv3, under **SNMPv3 Agent properties**, type the user name your network management tool uses to query the SMA appliance in the Username field.
8. To enable secure authentication, select the **Enable authentication (SHA-1)** check box, and type the password into the **Password** and **Confirm password** fields. MD5 is not supported, as SHA-1 is more secure.
9. To enable encryption for privacy, select the **Enable privacy (AES)** check box, and type the password into the **Password** and **Confirm password** fields. DES is not supported, as AES is more secure.
10. Under **SNMP Hosts**, define the management systems from which the appliance will allow SNMP requests. You can allow the request to come from any host by typing `0.0.0.0` for both the IP address and the subnet mask. Keep in mind, however, that the trade-off for this convenience is decreased appliance security.



SNMP HOSTS

Define one or more management systems from which the appliance will allow SNMP requests.

□	IP ADDRESS	NETMASK

No rows to display

    a. In the **SNMP hosts** area, click **New**.
    b. Type the **IP address** and a **Netmask** for the host, and then click **OK**.

11. Under **Trap receivers**, select the **Enable support for SNMP traps** check box to enable traps being sent. You can clear the check box to disable traps from being sent.

    If traps are enabled then all traps will be sent to all hosts defined in the list. If traps are disabled then the list of hosts will be ignored.
12. Define the management systems to which the appliance will send SNMP traps.
    a. In the **Trap receivers** area, click the **+** (New) icon.
    b. Type the **IP address** and a **Netmask** for the host, and then click **OK**.
13. Click **Save**.

Downloading the MIB File

AMC enables you to download the Secure Mobile Access MIB file, which adds VPN-specific data to already supported MIBs. See MIB Data for details on the information provided by the MIB.

To download the MIB:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Network Services** section, click the **Configure** link under **SNMP**.
3. Click the **Download MIB** button.

A file download message appears.

4. Click **Save**, browse to the correct directory, and then save the `SMA1000CustomMibs.tar` file.

Retrieving Management Data Using SNMP

SNMP data is arranged in a standardized hierarchy made up of structured text files that describe valuable management data. These text files (called MIBs) contain descriptions of specific data variables, such as system information or status.

ⓘ **NOTE:** For more information on MIB II (including an explanation of the MIB II variable names), see http://www.ietf.org/rfc/rfc1213.txt.

To retrieve information through SNMP, you query the system for an object identifier, or OID. Each OID includes a text name, but is usually referenced using a number. For example, the OID for system uptime (**sysUpTime**) is `1.3.6.1.4.1.8741.3`.

If you don't have an SNMP management package, you can retrieve SNMP data by connecting to the appliance, logging in as *root*, and then running the **snmpwalk** or **snmpget** command. For example, to retrieve information about disk space availability, you could type the following **snmpwalk** command to query OID

`1.3.6.1.4.1.2021.9`:

```
# snmpwalk -v 2c -c public localhost 1.3.6.1.4.1.8741.9
```

To view a list containing all MIB variables, type:

```
snmpwalk -v 1 -O n localhost -c public |more
```

This command returns a list like this:

```
.1.3.6.1.2.1.1.1.0 = Linux E-Class SMAvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50 PDT 2017
i686

.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.2021.250.10

.1.3.6.1.2.1.1.3.0 = Timeticks: (1707979) 4:44:39.79

.1.3.6.1.2.1.1.4.0 = Root < root@localhost> (configure /etc/snmp/snmp.local.conf)

.1.3.6.1.2.1.1.5.0 = E-Class SMAvpn

.1.3.6.1.2.1.1.6.0 = Unknown (configure /etc/snmp/snmp.local.conf)

.1.3.6.1.2.1.1.8.0 = Timeticks: (7) 0:00:00.07

.1.3.6.1.2.1.1.9.1.2.1 = OID: .1.3.6.1.2.1.31
```

To view a list containing all MIB names (which are helpful for use with the **snmpget** command) type:

```
snmpwalk -O S localhost -c public |more
```

This command returns a list like the following:

```
SNMPv2-MIB::sysDescr.0 = Linux E-Class SMAvpn 2.4.20_004 #1 SMP Thu Apr 10 14:35:50 PDT
2003

i686
```

```
SNMPv2-MIB::sysObjectID.0 = OID : SNMPv2-SMI::enterprises.2021.250.10

SNMPv2-MIB::sysUpTime.0 = Timeticks: (1712451) 4:45:24.51

SNMPv2-MIB::sysContact.0 = Root (configure /etc/snmp/snmp.local.conf)

SNMPv2-MIB::sysName.0 = E-Class SMAvpn

SNMPv2-MIB::sysLocation.0 = Unknown (configure /etc/snmp/snmp.local.conf)

SNMPv2-MIB::sysORLastChange.0 = Timeticks: (7) 0:00:00.07

SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB

..
```

MIB Data

The MIB modules reference object identifiers (OIDs) or text names that provide information about the SMA appliance; see the MIB data table.

MIB data	For more detailed information
System information	MIB Data: System Information Module
System health	MIB Data: System Health Module
Service health	MIB Data: Service Health
Security history	MIB Data: Security History Module
Network tunnel service	MIB Data: Network Tunnel Service Module
System traps	MIB Data: Traps
Other SNMP data	MIB Data: Other SNMP Data

MIB Data: System Information Module

The OIDs in the System Information module provide basic information about the appliance.

MIB Data: System Information Module

Item	OID	Description
Version	`1.3.6.1.4.1.674.1.1.0`	The version of Secure Mobile Access firmware running on this node in `major.minor.micro-hotfix-build` format (for example, `12.1.1.1-128`).

Hardware model	`1.3.6.1.4.1.674.1.2.0`	The model number of the appliance (for example, SMA 7200, SMA 7210, SMA 6200, and SMA 6210). New model numbers may be added in the future.

MIB Data: System Health Module

The OIDs in the System Health module provide information about the operational status of the appliance.

MIB Data: System Health Module

Item	OID	Description
Currently logged in	`1.3.6.1.4.1.674.2.1.1.0`	The number of currently authenticated active user sessions.
Maximum licensed users	`1.3.6.1.4.1.674.2.1.3.0`	The maximum number of active user sessions for which the appliance (or cluster of appliances) is licensed.
Current connections	`1.3.6.1.4.1.674.2.2.1.0`	The number of concurrent connections currently being serviced by the appliance (or cluster of appliances).
CPU utilization	`1.3.6.1.4.1.674.2.3.0`	The percentage of the CPU (or sum of CPUs, on a dual-processor machine) being used on a single appliance node over a time span of five seconds.
RAM utilization	`1.3.6.1.4.1.674.2.4.1.0`	The current virtual memory (RAM) percentage in use.
Swap utilization	`1.3.6.1.4.1.674.2.4.2.0`	The current virtual memory (swap) percentage in use.
Log utilization	`1.3.6.1.4.1.674.2.9.0`	The percentage of the log file disk partition being used.

Peak logged in	`1.3.6.1.4.1.674.2.1.2.0`	The maximum number of authenticated, active user sessions since the last reset; the reset interval is 24 hours.
Peak connections	`1.3.6.1.4.1.674.2.2.2.0`	The maximum number of concurrent appliance connections since the last reset; the reset interval is 24 hours.
Internal interface current throughput	`1.3.6.1.4.1.674.2.5.1.0`	Over a time span of five seconds, the current VPN throughput (inbound and outbound) in megabits per second as measured on the internal interface of the node.
Internal interface peak throughput	`1.3.6.1.4.1.674.2.5.2.0`	The peak VPN internal interface throughput (inbound and outbound) in megabits per second since the last reset.
External interface current throughput	`1.3.6.1.4.1.674.2.5.3.0`	Over a time span of five seconds, the current VPN throughput (inbound and outbound) in megabits per second as measured on the external interface of the node.
External interface peak throughput	`1.3.6.1.4.1.674.2.5.4.0`	The peak VPN external interface throughput (inbound and outbound) in megabits per second since the last reset.
Cluster interface current throughput	`1.3.6.1.4.1.674.2.5.5.0`	Over a time span of five seconds, the current mean average VPN cluster interface throughput (inbound and outbound) in megabits per second. The reset interval is 24 hours.

Cluster interface peak throughput	`1.3.6.1.4.1.674.2.5.6.0`	The peak VPN cluster interface throughput (inbound and outbound) in megabits per second since the last reset. The reset interval is 24 hours.

MIB Data: Service Health

The OIDs in the Service Health module shown in the below table provide information about the status of each service running on the appliance. For each service, the MIB provides a service ID, service description, and a service state of up or down.

MIB DATA: SERVICE HEALTH MODULE

Item	OID	Description
Service ID	`1.3.6.1.4.1.674.3.1.1.1.1`	The service ID for the AMC is 1
	`1.3.6.1.4.1.674.3.1.1.1.3`	The service ID for the SonicWall Web proxy service is 3
	`1.3.6.1.4.1.674.3.1.1.1.4`	The service ID for WorkPlace is 4
	`1.3.6.1.4.1.674.3.1.1.1.5`	The service ID for syslog-ng (the process that writes out the E-Class SMA appliance log files) is 5

Service description	`1.3.6.1.4.1.674.3.1.1.2.1`	Appliance Management Console (AMC)
	`1.3.6.1.4.1.674.3.1.1.2.2`	(Obsolete) Client /Server Access Service (AVPN)
	`1.3.6.1.4.1.674.3.1.1.2.3`	Secure Web access service (Workplace). This is also referred to as “Web proxy service”
	`1.3.6.1.4.1.674.3.1.1.2.4`	ASAP WorkPlace; this is the same as WorkPlace
	`1.3.6.1.4.1.674.3.1.1.2.5`	Syslog-ng (the process that writes out the E-Class SMA appliance log files)

Service state	`1.3.6.1.4.1.674.3.1.1.3.1`	The current state of AMC: 1 (up) or 2 (down)
	`1.3.6.1.4.1.674.3.1.1.3.3`	The current state of the Web proxy service: 1 (up) or 2 (down)
	`1.3.6.1.4.1.674.3.1.1.3.4`	The current state of WorkPlace: 1 (up) or 2 (down).
	`1.3.6.1.4.1.674.3.1.1.3.5`	The current state of syslog-ng: 1 (up) or 2 (down)

MIB Data: Security History Module

The OIDs in the Security History module provide information on login and access denials.

MIB Data: Security History Module

Item	OID	Description
Number of login denials	`1.3.6.1.4.1.674.4.1.0`	The number of login denials in the last 24 hours.
Last user denied login	`1.3.6.1.4.1.674.4.2.1.0`	The last user who was denied authentication, shown in the format `user@realm`.
Last denied login time	`1.3.6.1.4.1.674.4.2.2.0`	The time and date when the last user was denied authentication. The string is in the form `Wed May 30 21:49:08 2017`, in the same time zone for which the appliance is configured.

Number of access denials	`1.3.6.1.4.1.674.4.3.0`	The number of access denials in the last 24 hours.
Last user denied access	`1.3.6.1.4.1.674.4.4.1.0`	The last user who was denied access, shown in the format `user@realm`.
Last resource access denied	`1.3.6.1.4.1.674.4.4.2.0`	The `URL, host:port` or `host` of the last resource to which access was denied.
Last access denied time	`1.3.6.1.4.1.674.4.4.3.0`	The time and date when the last user was denied access. The string is in the form `Wed May 30 21:49:08 2017`, in the same time zone for which the appliance is configured.

MIB Data: Network Tunnel Service Module

The OIDs in the NG Server module provide information status of the network tunnel service.

MIB Data: Network Tunnel Service Module

Item	OID	Description
NG server state	`1.3.6.1.4.1.674.5.1.0`	The current state of the network tunnel service: Active, Down, or Crashed
Number of client address pools	`1.3.6.1.4.1.674.5.2.0`	The number of client address pools assigned to the network tunnel service
Client address pool range table	`1.3.6.1.4.1.674.5.3`	A table showing how many IP address pools are currently active and their IP address ranges
Client address pool entry	`1.3.6.1.4.1.674.5.3.1`	The number of currently active IP address pools
Client address pool utilization	`1.3.6.1.4.1.674.5.3.1.2.0`	Percentage of virtual IP addresses (VIPs) that are issued from a client address pool

Client IP address pool start range	`1.3.6.1.4.1.674.5.3.1.3.0`	The starting IP address of a client IP address pool range
Client address pool end range	`1.3.6.1.4.1.674.5.3.1.4.0`	The ending IP address of a client IP address pool range
Number of NG SLL tunnels	`1.3.6.1.4.1.674.5.4.0`	Total number of active network tunnels
SSL tunnel table	`1.3.6.1.4.1.674.5.5`	A table showing network tunnel statistics
SSL tunnel ID	`1.3.6.1.4.1.674.5.5.1.1.0`	An ID number assigned to a network tunnel session
SSL tunnel user	`1.3.6.1.4.1.674.5.5.1.2.0`	The user name associated with a network tunnel session
SSL tunnel VIP	`1.3.6.1.4.1.674.5.5.1.3.0`	The virtual IP address (VIP) associated with a network tunnel session
Number of flows per tunnel	`1.3.6.1.4.1.674.5.5.1.4.0`	The number of data flows in a network tunnel session
SSL Tunnel Uptime	`1.3.6.1.4.1.674.5.5.1.5.0`	1.3.6.1.4.1.674.5.5.1.5.0 Uptime statistics for a network tunnel session

MIB Data: Traps

A trap is a message the SNMP agent sends to indicate that a significant event has occurred that needs an administrator’s attention. To download the Secure Mobile Access MIBs, click **Services** in the main navigation menu, and then click **Configure** in the SNMP area. Click **Download MIB** to save a copy of the file (`SMA1000CustomMibs.tar`).

MIB Data: Traps

Item	MIB filename	Description
ngServerStateChange	*SonicWallNGServer*	The server core functionality depends on user space processes (*avssld* and *avpsd*) and two *avevent* kernel threads. The SNMP agent monitors these processes and when any of these go down this trap is triggered. The trap description specifies the component; for example, *avssld(0)*.

ngclientAddrPoolUtilizationWarning	*SonicWallNGServer*	This trap is triggered when the use of the client address pool exceeds the threshold.
asapServiceUp	SonicWallServiceHealth	A service on a single node system, identified by the IP address from which the trap is sent, is up. The *serviceDescription* OID is sent along with the trap.
asapServiceDown	SonicWallServiceHealth	A service on a single node system, identified by the IP address from which the trap is sent, has gone down. The *serviceDescription* OID is sent along with the trap.
cpuCapacityWarning	SonicWallSystemHealth	The heuristically determined percentage of CPU capacity used on a single node system has exceeded the capacity for a single node (*cpuCapacityUtilization*). *cpuCapacityUtilization* OID is sent along with the trap.
memoryCapacityWarning	SonicWallSystemHealth	The heuristically determined percentage of memory capacity used on a single node system has exceeded 90 percent of capacity (*memoryCapacityUtilization*). memoryCapacityUtilization OID is sent along with the trap.
logCapacityWarning	SonicWallSystemHealth	The percentage of log file disk space used on a single node system has exceeded 90 percent of the total capacity. logUtilization OID is sent along with the trap.
userLimitWarning	SonicWallSystemHealth	Notification is generated if the concurrent number of authenticated users on a single node system (*currentlyLoggedIn*) has reached 90 percent of the license capacity limit. currentlyLoggedIn OID is sent along with the trap.
userLimitReached	SonicWallSystemHealth	The number of currently authenticated, active user sessions on a single node system (*currentlyLoggedIn*) has reached the current license capacity limit. currentlyLoggedIn OID is sent along with the trap.
userLimitExceeded	SonicWallSystemHealth	The number of concurrent, authenticated users on a single node system has reached the current license capacity limit (*currentlyLoggedIn*) for authorized users. currentlyLoggedIn OID is sent along with the trap.
asapSystemUp	SonicWallSystemInfo	For a single appliance (not in an HA pair): the appliance from which the notification is sent (identified by IP address) is back online.

asapSystemDown	SonicWallSystemInfo	For a single appliance (not in an HA pair): the appliance from which the notification is sent (identified by IP address) is going offline.

MIB Data: Other SNMP Data

The MIB Data: Other SNMP data table shows some other information about the appliance that you can retrieve from the standard MIB file using SNMP.

MIB Data: Other SNMP Data

Item	OID	Description
Service status table	`1.3.6.1.4.1.674.2`	Checks the status of any of the following services. The return data references the following process names. If a process status is listed as not running, an error is flagged. • apache2 (Web proxy service) • logserver (log server) • syslog-ng (syslog) • policyserver (policy server) In appliance version 8.9.0 and later, srvcmond (cluster manager) is replaced with a service named AVFM (Secure Mobile Access Flow Manager). AVFM does not appear in a process list on the appliance because it is run as a kernel module.
Disk space availabilitytable	`1.3.6.1.4.1.674.9`	Checks disk space availability for the following partitions: “/”, “/var/log”, and “/upgrade”. If the disk space on a partition drops below 10MB, an error is flagged.
Load average checks table	`1.3.6.1.4.1.674.10`	Checks the load average for intervals of one, five, or 15 minutes. An error is flagged if the load average is greater than 12 at the one-minute interval, or greater than 14 for the five- and 15-minute intervals.
Software version number table	`1.3.6.1.4.1.674.50`	Checks the current version of the SonicWall system software.
System name	`1.3.6.1.4.1.674.0`	Checks the name of the system.

Managing Configuration Data

The configuration data for your appliance is stored in a single export archive (`.aea`) file that includes the types of configuration data shown in the Configuration Data types table.

Configuration Data Types

Type of configuration data	Description
Access policy	Rules, resources, users and groups, WorkPlace shortcuts, and EPC signatures and zones.
Certificates	Certificates, private keys, and certificate passwords.
WorkPlace customization	General appearance settings, custom content, and custom templates.

It's a good practice to back up the configuration data on your appliance, especially if you are working on system changes and may need to revert to an earlier configuration. For example, if you plan to add new access control rules, first save your configuration, and then make your changes: you can then revert to the saved (working) configuration if the new rules don't work as expected.

There are several options for saving and restoring configuration data:

- Export configuration data to a local machine, and later import it. Exporting involves the complete set of configuration data, but it is possible to do just a partial import. See Exporting the Current Configuration to a Local Machine and Importing Configuration Data for more information.
- Save and restore configuration data files on the appliance. This involves the complete set of configuration data: you cannot save or restore a partial configuration. For more information, see Saving the Current Configuration on the Appliance and Deleting or Restoring or Exporting Configuration Data Stored on the Appliance.
- You can export the policy from an older SonicWall Secure Mobile Access appliance and import it to a newer one, provided the older appliance, in general, predates the newer one by no more than three versions. See the *SMA 12.4.2 Upgrade Guide* for information on supported platforms and see Updating the System for a description of the version number conventions that SonicWall uses.

⚠ | **CAUTION: Only configuration data that was generated by AMC is saved or exported.**

Topics:

- Exporting the Current Configuration to a Local Machine
- Saving the Current Configuration on the Appliance
- Importing Configuration Data
- Deleting or Restoring or Exporting Configuration Data Stored on the Appliance
- Saving and Restoring Configuration Data

Exporting the Current Configuration to a Local Machine

You can export your complete set of appliance configuration data to a local machine. Only saved changes are included; changes that are pending when you export a configuration are discarded.

ⓘ | **NOTE:** You cannot extract readable configuration data from .aea files.

You can enable to include third party agents to export the configuration of third party agents such as, Citrix and VMware View clients.

To export the current configuration:

1. In the AMC, navigate to **System Configuration > Maintenance**.
2. In the **System Configuration** section, click **Import/Export**.
3. Click **Export**.

   The **Export Configuration** page displays, and a **File Download** prompts you to open the `SonicWallSMAAppliance-_<firmware version><date>-<nnn>.aea` file or save it to your hard drive. For example: `virtual98.sea.eng.sonicwall.com_12.4.2-05073_20220629-201659`.
4. Click **Save**, browse to the correct directory, and then save the `.aea` file.
5. Click **OK** on the **Export** page.

Importing Configuration Data

Exporting always involves the complete set of configuration data, but it is possible to do just a partial import (for example, if you want to import only policy and WorkPlace settings).

The below table describes the types of data that you can import into an existing AMC configuration:

Configuration Data For Importing

Type of configuration data	Description
Partial configuration	• **Access policy**: Includes rules, resources, users and groups, and EPC device profiles and zones. • **WorkPlace customization**: Includes general appearance settings, custom content, shortcuts, and custom templates. • **CA certificates**: Includes the CA certificates that are used to secure authentication server connections, or back-end Web resources, with SSL. • **End Point Control**: If you use client certificates in device profiles, a partial configuration includes the CA that issued them to your users.
Entire configuration	• Partial configuration data (see the *Partial configuration* table). • **SSL certificates**: Includes certificates for AMC and the appliance, along with private keys and passwords.

To import a full or partial configuration:

1. From the main navigation menu, click **Maintenance**.
2. In the **System configuration** area, click **Import/Export**.
3. In the **File name** box, type the path of the appropriate file (`SonicWallSMAApplianceVPN-<date>-<nnn>.aea`), or click **Browse** to locate it.
4. Click **Partial configuration** if you want to import just the items listed in the table above.
5. Click **Import**. To activate the imported configuration, you must apply changes. See Applying Configuration Changes for more information.

ⓘ | **NOTE:**

- If an import fails, you can view details in the `Management message log` file.
- If you import a configuration while other configuration changes are pending in AMC, the pending changes are overwritten.
- You can import the policy from an older Secure Mobile Access appliance, provided the older appliance predates the newer one by no more than three versions. For example, you cannot import the policy configuration from versions earlier than 12.1 to your 12.4 appliance.

Saving the Current Configuration on the Appliance

In contrast to exporting, saving configuration data stores it on your appliance (up to 20 saved configurations can be stored). You cannot save a partial configuration, and only changes that have been applied are included.

To save configuration data on the appliance:

1. In the AMC, navigate to **System Configuration > Maintenance**.
2. In the **System Configuration** area, click **Import/Export**.
3. Click the **+** (New) icon in the **Saved Configurations** list.
4. Describe this configuration in the **Description** field and (if there are multiple administrators) it is a good practice to identify who is saving it.

   For example, an entry might read as follows: `Saved by MIS before adding access control rules for mobile devices.`
5. Click **Save**.

   The current configuration data is stored on the appliance and added to the **Saved Configurations** list.

Deleting or Restoring or Exporting Configuration Data Stored on the Appliance

Follow these steps to delete or restore or export a configuration file that is stored on the appliance. (To specify configuration data that is stored on a local machine instead of the appliance, use the import feature. See Importing Configuration Data for more information.) Only a full configuration data file can be restored; you cannot restore a partial configuration.

To delete or restore or export configuration data stored on the appliance:

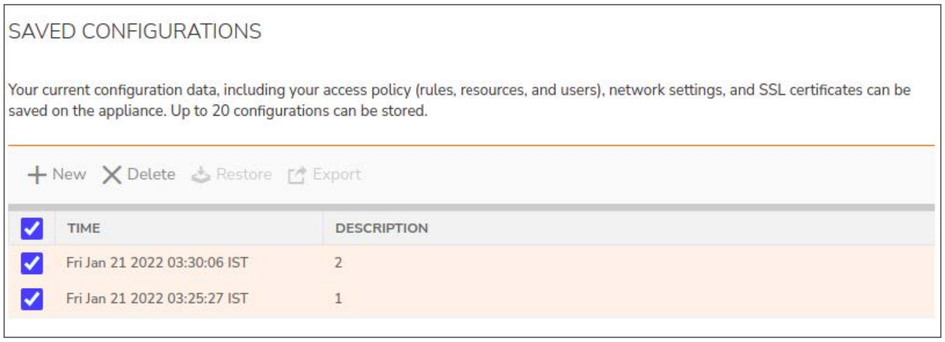
1. In the AMC, navigate to **System Configuration > Maintenance**.
2. In the **System Configuration** area, click **Import/Export**.
3. Select a configuration from the **Saved Configurations** list.
4. Delete or restore or export the configuration to a local machine:

- Click **Delete** to delete the saved configuration from the appliance.
- Click **Restore**. Restoration of the selected configuration begins immediately. After the restore is complete, click **Pending changes** to apply the new configuration.

  The restored configuration remains in the list.
- Click **Export** to save a copy of the configuration to a local machine. See the Exporting the Current Configuration to a Local Machine section.

  ⓘ | **NOTE:**

  - The options to **Delete**, **Restore** and **Export** saved configuration is enabled when a single configuration is selected.
  - When multiple configurations are selected, **Restore** and **Export** is graded out and **Delete** option is enabled.



SAVED CONFIGURATIONS

Your current configuration data, including your access policy (rules, resources, and users), network settings, and SSL certificates can be saved on the appliance. Up to 20 configurations can be stored.

☑	TIME	DESCRIPTION
☑	Fri Jan 21 2022 03:30:06 IST	2
☑	Fri Jan 21 2022 03:25:27 IST	1

Upgrading, Rolling Back, or Resetting the System

SonicWall periodically offers software updates that add new functionality or address existing issues. An update is delivered as a compressed `.bin` file and can be in the form of:

- A *hotfix*, which addresses issues with a particular version of the appliance software and typically contains only the files that have changed from the original version.
- An *upgrade*, which is a new version of the software (the version number on the appliance is incremented).

Installing either kind of update, or rolling back to a previous version, can be done using AMC.

To view the current version of the system, click **System Status** or **Maintenance** from the main navigation menu. If any hotfixes have been applied, you can view the list by clicking the **hotfixes** link.

ⓘ | **NOTE:** AMC now notifies the administrators of available upgrades and hotfixes, and provides a one-click upgrade option.

Topics:

- Updating the System
- Rolling Back to a Previous Version
- Resetting the Appliance

Updating the System

You can find system updates (hotfixes and upgrades) on the MySonicWall Web site. To access www.mysonicwall.com, you must first create an account, which is described in Creating a MySonicWall Account. After you have an account, new system updates and documentation are available in the **Download Center** on the Web site.

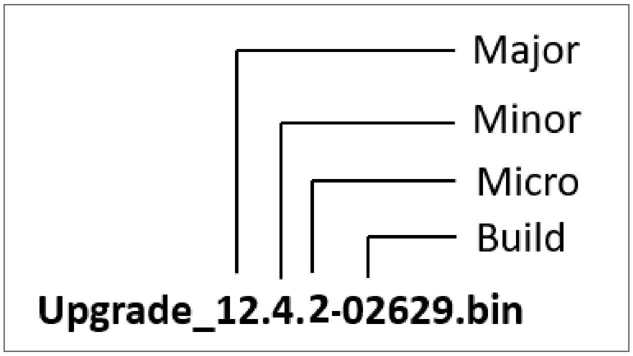
Topics:

- Naming Conventions for Upgrades
- Naming Conventions for Hotfixes
- Installing System Updates

Naming Conventions for Upgrades

SonicWall uses this syntax, described in below table to describe version numbers for upgrade files:

```
upgrade-<major>.<minor>.<micro>-<build>.bin
```



ⓘ **NOTE:** To find out if any hotfixes have been applied, click **System Status** or **Maintenance** from the main navigation menu.

The version number for AMC (displayed in the bottom-left corner of every AMC page) and client software follows a similar pattern:

```
<major>.<minor>-<micro>-<build>
```

Naming Conventions For Upgrades

Name	Description
major	The major release number. If this is the only number that is present, it indicates that this release contains significant new features plus fixes. It also indicates that it contains a full image of the entire system.
minor	The minor release number. If the version number contains only the major and minor numbers, it indicates that this release contains incremental features plus fixes. It also indicates that it contains a full image of the entire system.

micro	The micro release number. If the version number contains only the major, minor, and micro numbers, it indicates that this release contains a small number of features plus fixes. It also indicates that it contains a full image of the entire system.
build	An internal build number used by SonicWall. All releases contain a build number.

Naming Conventions for Hotfixes

Between releases, SonicWall may issue a hotfix that replaces a subset of the software files on your SMA appliance. Hotfix filenames use this naming convention:

```
<component>-hotfix-<version>-<hotfix number>
```

where the below table defines `<component>`.

Naming Conventions For Hotfixes

Component	Description
Pform	Appliance Management Console
clt	Client software

ⓘ **NOTE:** To check whether any hotfixes have been applied, click **System Status** or **Maintenance** from the main navigation menu. If any hotfixes have been incorporated, you'll see a **hotfixes** link next to the version number. Click the link for more information about which ones have been applied.

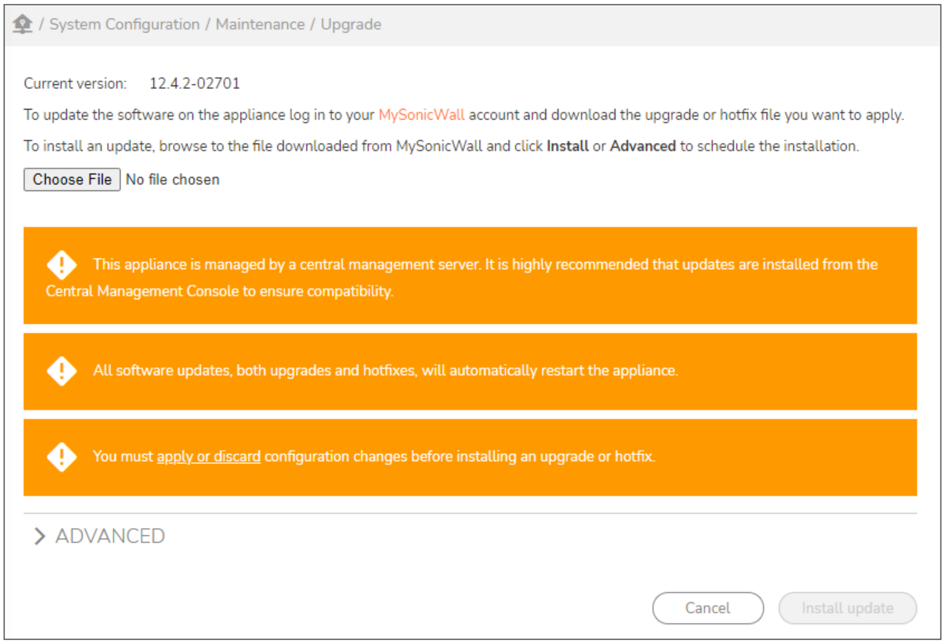
For example, `Pform-hotfix-12.4.0-001` is hotfix 001 for version 12.4 that fixes a problem in Appliance Management Console.

Installing System Updates

You can use AMC to install version upgrades and hotfixes manually or automatically at a scheduled time.

To download and install a system upgrade or hotfix manually:

1. In the AMC, navigate to **System Configuration > Maintenance**.
2. In the **System software updates** area, click **Update**.



Current version: 12.4.2-02701

To update the software on the appliance log in to your MySonicWall account and download the upgrade or hotfix file you want to apply.

To install an update, browse to the file downloaded from MySonicWall and click **Install** or **Advanced** to schedule the installation.

This appliance is managed by a central management server. It is highly recommended that updates are installed from the Central Management Console to ensure compatibility.

All software updates, both upgrades and hotfixes, will automatically restart the appliance.

You must apply or discard configuration changes before installing an upgrade or hotfix.

3. If you have not already downloaded the upgrade or hotfix file, click the Web site link (login required) and download the appropriate file from www.mysonicwall.com to your local file system.
4. Type the path of the file, or click **Browse** to locate it.
5. Click **Install Update**.

   A file upload status indicator appears. If necessary, you can click **Cancel** to stop the upload process.

   After the file upload process is complete, the update is automatically installed on the appliance. You cannot cancel the installation process. After the installation process is complete, the appliance automatically restarts.
6. After the appliance restarts, log in to AMC and verify the new version number in the bottom-left corner of the AMC home page.

ⓘ **NOTE:** If you see an error message indicating that a upgrade file is invalid or corrupt, follow the steps in Verify a Downloaded Upgrade File to see if the checksum for the file is correct.

Rolling Back to a Previous Version

From AMC, you can undo the most recent update installed on the system. If you experience problems after installing an upgrade or hotfix, you may want to use this feature to roll back to a known state. Each time you roll back, the most recent update is removed.

△ **CAUTION: If you have made any configuration changes since you updated the appliance they will be lost if you restore a previous version of the system software. When you remove a hotfix, on the other hand, your configuration changes are preserved.**

To roll back to a previous version:

1. In the AMC, navigate to **System Configuration > Maintenance**.
2. In the **System configuration** area, click **Rollback**.
3. To roll back to the version displayed on the **Rollback** page, click **OK**.

   After the rollback process is complete, the appliance automatically restarts and applies the changes.
4. After the appliance restarts, verify the new version number in the bottom-left corner of the AMC home page.

Resetting the Appliance

From AMC, you can reset your appliance using one of three reset levels. The mildest level erases your configuration information, log files, and the current firmware, but leaves you the option to roll back to a previous version, if one is loaded.

The second level removes all configuration, log files, and firmware from the appliance. With this option, you cannot roll back to a previous version.

The third level also removes all configuration, log files, and firmware from the appliance, and then securely erases the hard drive, which can take up to 45 minutes.

There are a couple of scenarios in which a reset may be appropriate:

- You want to completely clean the machine and reuse it elsewhere.
- The appliance is in an unrecoverable state. In this case, you should contact SonicWall Technical Support and confirm that there is no other solution to your problem. A reset should be used only as a last resort to restore the appliance to a working condition.

To configure the appliance after it has been reset, you will need to use the LCD panel or serial console.

To reset the appliance:

1. Back up the configuration data on the appliance. You can do this:
   - In AMC (see Exporting the Current Configuration to a Local Machine).
   - By using Backup Tool (see Saving Configuration Data).
2. In the AMC, navigate to **System Configuration > Maintenance**.
3. In the top section of the page, click **Reset**.
4. On the **Maintenance > Reset** page, select one of the following three radio buttons under **Reset Options**:
   - **Reset the current configuration** – This option erases your current configuration. If you upgraded from a previous version, selecting this option retains the ability to roll back.
   - **Reset the entire appliance** – This option erases your configuration and deletes all firmware versions on the appliance. If you select this option, you cannot roll back to a previous version.
5. At the bottom of the page, click **Reset** to proceed with the reset. To cancel the reset, click **Cancel**.

To reset the appliance with a different version of the firmware:

ⓘ **NOTE:** The purpose of the firmware downgrade capability is to permanently "downgrade" an appliance to a different base firmware version therefore it does **NOT** migrate the existing configuration or save any data or files from the appliance. It is the equivalent of a complete factory reset to an entirely new firmware base. All files and settings stored on the appliance will be permanently overwritten and the appliance will be set to factory defaults.

For more information and instructions on how to perform a firmware downgrade, see https://www.sonicwall.com/en-us/support/knowledge-base/170502558229507.

Permanently Disabling the Appliance

You also have the ability to permanently disable an appliance by deleting all firmware versions on the appliance and securely erasing the contents of its hard drive.

⚠ **WARNING: This procedure will leave the appliance in a permanently unusable state. All firmware versions will be deleted, and the hard drive will be securely erased.**

△ **CAUTION: This is a destructive operation and cannot be undone. If you need to preserve your current configuration, make sure that you have exported it before continuing.**

To permanently disable the appliance:

1. Access the advanced settings by following the instructions provided here: https://www.sonicwall.com/en-us/support/knowledge-base/170502558229507.
2. Select **Securely erase the hard drive and permanently disable the entire appliance**.

   This option erases your configuration, deletes all firmware versions, and securely erases the hard drive.

   ⓘ **NOTE:** Securely erasing the hard drive can take up to 45 minutes.
3. Enter `CONFIRM` in the field provided.
4. Click **Reset**.

SSL Encryption

Encryption is used to ensure data security for all traffic on the appliance. The appliance encrypts all data using SSL. In **System Configuration** > **SSL Settings**> **Security Level** section, select the version of TLS transport protocol that the appliance uses.

ⓘ **NOTE:** By default, the TLS transport protocol is set as Secure.

- Modern: Supports TLS 1.3 only. Provides the highest level of security without providing backward compatibility for older clients.
- Secure: Supports only secure protocols (TLS 1.2 and higher) and ciphers. Recommended for most systems, provides the best balance of security and compatibility.
- Legacy : Adds support for older ciphers that are no longer considered secure (TLS 1.2 and higher).

Configuring SSL Encryption

The appliance uses SSL encryption and other cryptographic algorithms-or ciphers-to secure data transfer. The default settings are typically sufficient for most deployments.

Secure Mobile Access has been enhanced to support TLS 1.3 for incoming and outgoing connections, which is the latest and more secure TLS version.

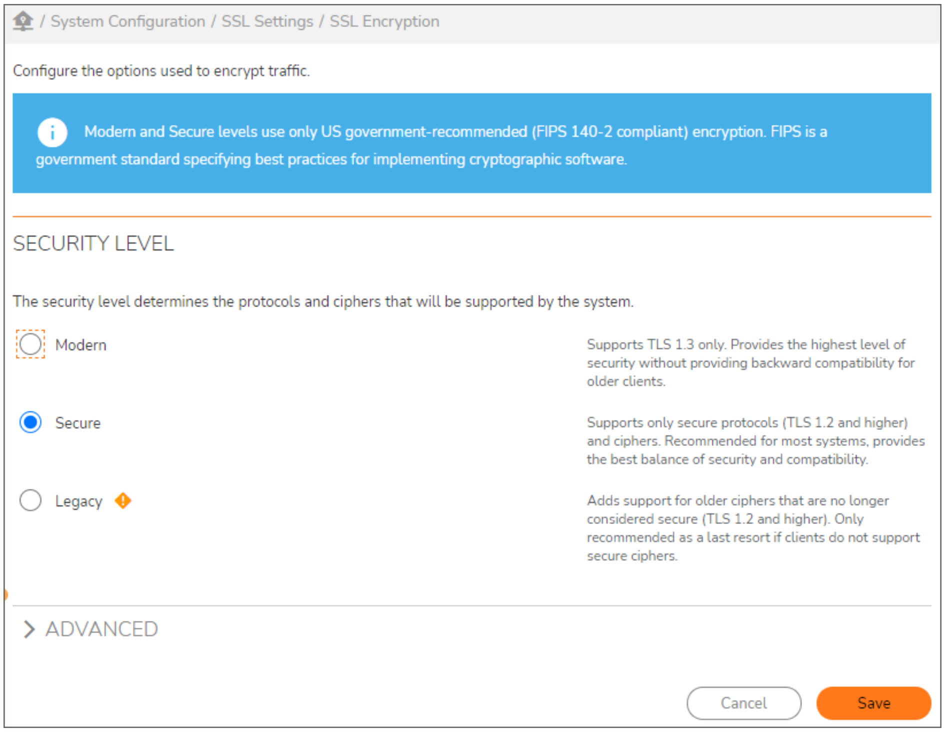
> ⓘ **NOTE:** TLS 1.0 and TLS 1.1 are no longer supported for user sessions and supported only for outgoing connections to legacy internal resources.

> ⓘ **NOTE:** If you have configured TLS transport protocol as “Any TLS version” or “TLS version 1.2 or 1.1” in prior version of SMA, upgrading to SMA 12.4 is prevented. To upgrade to SMA 12.4, select “TLS version 1.2 only” in AMC and proceed with the upgrade process.

To configure SSL encryption settings:

1. In the AMC, navigate to **System Configuration > SSL Settings**.
2. Click the **Edit** link in the **SSL Encryption** section.

   The **SSL Encryption** page displays.



/ System Configuration / SSL Settings / SSL Encryption

Configure the options used to encrypt traffic.

Modern and Secure levels use only US government-recommended (FIPS 140-2 compliant) encryption. FIPS is a government standard specifying best practices for implementing cryptographic software.

SECURITY LEVEL

The security level determines the protocols and ciphers that will be supported by the system.

○ Modern — Supports TLS 1.3 only. Provides the highest level of security without providing backward compatibility for older clients.

● Secure — Supports only secure protocols (TLS 1.2 and higher) and ciphers. Recommended for most systems, provides the best balance of security and compatibility.

○ Legacy — Adds support for older ciphers that are no longer considered secure (TLS 1.2 and higher). Only recommended as a last resort if clients do not support secure ciphers.

> ⓘ **NOTE:** All security levels use only US government-recommended (FIPS 140-2 compliant) encryption. FIPS is a government standard specifying best practices for implementing cryptographic software. This configures the appliance to use only the TLS protocol and enables only FIPS-compliant ciphers.

3. In the **Security Level** section, select the version of TLS transport protocol that the appliance will use.

ⓘ | **NOTE:** By default, the TLS transport protocol is set as Secure.

a. **Modern**: Supports TLS 1.3 only. Provides the highest level of security without providing backward compatibility for older clients.

    - Modern TLS transport protocol supports the following ciphers/suites.

        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384

b. **Secure**: Supports only secure protocols (TLS 1.2 and higher) and ciphers. Recommended for most systems, provides the best balance of security and compatibility.

    - Secure TLS transport protocol supports the following ciphers/suites.

        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

c. **Legacy** : Adds support for older ciphers that are no longer considered secure (TLS 1.2 and higher).

    ⓘ | **NOTE:** The Legacy security level includes support for ciphers that are insecure, but are included only for compatibility with older browsers and clients.

    - Legacy TLS transport protocol supports the following ciphers/suites.

        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA

4. In case, if you want to use a different security level for connections to internal systems such as authentication servers (AD/LDAP), SMTP servers, and so on:

    a. In the Advanced section, select **Use a different security level for connections to internal systems** check box.

    b. In the **Internal security level** drop-down, select any one of the following:

        - **Modern**: Supports TLS 1.3 only. Provides the highest level of security without providing backward compatibility for older clients.

    - Modern TLS transport protocol supports the following ciphers/suites.
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
- **Secure**: Supports only secure protocols (TLS 1.2 and higher) and ciphers. Recommended for most systems, provides the best balance of security and compatibility.
    - Secure TLS transport protocol supports the following ciphers/suites.
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- **Legacy**: Adds support for older ciphers that are no longer considered secure (TLS 1.2 and higher).

  ⓘ **NOTE:** The **Legacy** security level includes support for ciphers that are insecure, but are included only for compatibility with older browsers and clients.

    - Legacy TLS transport protocol supports the following ciphers/suites.
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA
- **Obsolete**: If your TLS version is 1.1 or 1.0, however it is not recommended to use TLS 1.0 and 1.1 version.

5. Select the ciphers that the access services (Web proxy, network proxy, and network tunnel) on the appliance will accept for SSL connections.
    - **Provide the highest level of security**: Prefer 256-bit ciphers
    - **Allow the highest level of performance and capacity**: Prefer 128-bit ciphers
6. Click **Save**.

FIPS Certification

This section describes configuring your SMA appliance to use FIPS mode.

FIPS (Federal Information Processing Standard) 140-2 Level 2 is a validation standard for evaluating cryptographic modules, and includes stringent reviews of source code, algorithms, physical security, and operational testing on cryptographic security products. The United States Federal Government is required to purchase cryptographic products validated to the FIPS 140-2 standard. In the international marketplace, ISO19790 is being adopted as a standard and is a direct adaptation of FIPS 140-2.

The SonicWall SMA 7210,6210, and 8200v appliances are submitted for FIPS 140-2 Level 2 certification from NIST (the National Institute of Standards and Technology, the United States FIPS 140-2 Cryptographic Module Validation Authority) and CSE (the Communications Security Establishment, the Canadian FIPS 140-2 Cryptographic Module Authority).

ⓘ | **NOTE:** SMA 12.4 6210, 7210, 7200 and 8200v are FIPS certified.

FIPS mode is transparent to end users. Internally, FIPS mode enforces secure communication and system integrity.

Topics:

- Requirements for FIPS
- Managing FIPS-Compliant Certificates
- FIPS Violations
- Enabling FIPS
- Exporting and Importing FIPS-Compliant Certificates
- Disabling FIPS
- Zeroization

Requirements for FIPS

These items are required to properly configure FIPS for full compliance:

- An SMA 7200, 7210,6200, 6210, and 8200v appliance. No other appliances are FIPS-certified.

  △ | **CAUTION: If you have purchased an SMA 7200, 7210,6200, 6210, and 8200v appliance with 140-2 Level 2 FIPS certification.**
- A license to run FIPS
- A secure connection to your authentication server
- A strong administrator password, which should be at least 14 characters long and contain punctuation characters, numbers, and a combination of uppercase and lowercase letters.

These states prevent FIPS from being activated, or from reaching full compliance:

- Unsecured connections with authentication servers
- Use of RADIUS authentication servers
- Use of LDAP authentication servers without using SSL connections employing only FIPS approved ciphers

- Use of Active Directory single domain authentication servers without using SSL connections employing only FIPS approved ciphers
- Use of RSA Authentication Manager authentication servers without strong passwords as shared secrets
- Use of USB devices for any purpose
- Installation of third party software via the shell command line
- Use of Debug 1, Debug 2, Debug 3 or plaintext logging
- Use of certificates with private/public key-pairs generated by a non-FIPS-compliant system
- Use of the zeroization procedure without the primary administrator being physically present until the procedure completes; see Zeroization

FIPS mode is not automatically enabled after you import your license. You must set it up as described in Enabling FIPS.

Managing FIPS-Compliant Certificates

Any keys generated on an 7200, 7210,6200, 6210, and 8200v appliance running in FIPS mode will be FIPS compliant. If you import certificates (and their associated public and private keys) to the appliance, it is your responsibility to make sure that they are also FIPS compliant. Certificates must be exported and then reimported when you switch FIPS mode on or off. For the export and import procedure, see Exporting and Importing FIPS-Compliant Certificates.

The best way to ensure that the certificates you're using are FIPS compliant is to generate all CSRs (certificate signing requests) on a FIPS-enabled appliance.

FIPS Violations

Your appliance validates its integrity several ways:

- A self test is performed at each power-on cycle to verify all FIPS approved cryptographic algorithms are functioning properly. If any of the self tests fail, the **Alarm LED** on the front panel will remain lit, a message detailing the specific failure will be displayed on the serial console and logged in `/var/log/aventail/fips.log`, and the appliance will be halted. You should power-cycle the appliance once to see if it recovers. If it does not, you will need to contact SonicWall Customer Support for further instructions.
- A continuous self test is performed on the random number generator and on the generation of new Certificate keys to verify the integrity of cryptographic operations. If any of these self tests fail, a message detailing the specific failure will be displayed on the serial console and logged in `/var/log/aventail/fips.log`, and the appliance will be immediately power-cycled via a reboot in order to perform the rigorous self-tests for system integrity.
- All critical security binaries are signed and hashed. Prevent the alterations to signed files and the binaries are detected at each reboot and immediately on a running system. If this occurs during the power-cycle self tests, the **Alarm LED** on the front panel will remain lit, a message detailing the specific tampering will be displayed on the serial console and logged in `/var/log/aventail/fips.log`, the system will be halted and you will need to contact SonicWall Customer Support for further instructions. If this tampering

is detected on a running system, the appliance will be immediately power-cycled via a reboot in order to perform the rigorous self-tests for system integrity.

- All critical security configuration files are signed and hashed. Manual alterations are prevented by file locking (as opposed to alterations made using the AMC) and the configuration files causing the appliance to immediately transition into an error state are prevented. If this tampering is detected on a running system, the appliance will be immediately power-cycled via a reboot in order to perform the rigorous self-tests for system integrity. Otherwise, if it is detected during power-cycle self-tests, a message detailing the specific tampering will be displayed on the serial console and logged in `/var/log/aventail/fips.log`, the **Test LED** on the front panel remain lit and the system will be placed in single user mode with networking disabled. The primary administrator will need to log in via the serial console and restore tampered configuration files with valid backup copies or perform a configuration reset prior to power-cycling the appliance.

Enabling FIPS

Before you enable FIPS mode, you must have a strong password, a secure connection to your authentication server, and a valid license.

Obtain your FIPS license as described in Software Licenses.

To be FIPS-compliant, your password must be at least 8 characters long, but it is recommended that you use at least 14 characters. Although this requirement is not enforced by the software, having a weak administrator password leaves you vulnerable. A strong password includes a mix of letters, numbers and symbols. Think of this as a phrase, not just a password. For instance, `I never saw @ purple cow, I never hope 2C1` has a combination of all three types of characters.

To use your existing, FIPS-compliant certificates while in FIPS mode, export the certificates before enabling FIPS and then import them again after FIPS is enabled. See Exporting and Importing FIPS-Compliant Certificates.

To enable FIPS:

1. In the AMC, navigate to **General Settings > FIPS Security**.
2. Click **Edit**.
3. If you have imported your license, select the **Enable FIPS mode** checkbox.

   ⓘ **NOTE:** Existing certificates will be deleted from the system in the next step. To preserve your FIPS-compliant certificates, ensure that you have exported them.
4. Click **Save** and then apply your Pending changes.

   △ **CAUTION: When in FIPS mode, you cannot edit system configuration files.**

If your appliance configuration is not FIPS-compliant, in the upper-right corner you will see an alert link that says **FIPS-compliance warning**. Click on the link for more information on how to bring your appliance configuration into FIPS-compliance.

△ **CAUTION: The lack of this alert does not mean your environment is FIPS compliant. It is your responsibility to ensure all FIPS prerequisites are met in order to be FIPS compliant.**

Exporting and Importing FIPS-Compliant Certificates

If you know your existing Certificate keys were generated on a FIPS-compliant system and you want to use them after FIPS is enabled, you must export them before enabling FIPS and then import them after FIPS is enabled.

Similarly, if you plan to disable FIPS mode on your system and you want to use your FIPS-compliant certificates after disabling FIPS, you must export them before disabling FIPS and then import them after FIPS is disabled.

To export Certificates before the FIPS-mode transition:

1. In the AMC, navigate to **System Configuration > SSL Setting > SSL Certificates**.
2. For each certificate to export, do the following:
   a. On the **Certificates** table, select a certificate and click the **Export** button.
   b. Enter a password for encrypting the exported `.p12` file.
   c. Click the **Save** button.

To import certificates after the FIPS-mode transition:

1. In the AMC, navigate to **System Configuration > SSL Settings > SSL Certificates**.
2. For each certificate to import:
   a. On the **Certificates** table, select the **+** (New) icon
   b. Select **Import certificate** from the dropdown list.
   c. Select the certificate file to import.
   d. Enter the password with which the `.p12` file was encrypted.
   e. Click the **Import** button.

Disabling FIPS

Turning off FIPS disables the FIPS feature and removes all constraints imposed by the FIPS mode prerequisites.

> △ **CAUTION: Warning: To be fully FIPS compliant, no FIPS critical security parameters can be used outside of the FIPS approved mode of operation. A few of these parameters are burned into the firmware itself and thus to be fully compliant, zeroization must be performed. If you wish to continue using your system rather than returning the hardware to SonicWall for zeroization, and you are willing to knowingly skip zeroization, you can disable FIPS mode in the AMC. This will logically destroy all configurable parameters.**

To use your existing, FIPS-compliant certificates after disabling FIPS mode, export the certificates before disabling FIPS and then import them again after FIPS is disabled. See Exporting and Importing FIPS-Compliant Certificates.

To disable FIPS:

1. In the AMC, navigate to **System Configuration > General Settings**
2. In the **FIPS Security** section, click **Edit**.
3. Clear the box next to **Enable FIPS mode**.

   ⓘ | **IMPORTANT:** Existing certificates will be deleted from the system in the next step. To preserve your FIPS-compliant certificates, ensure that you have exported them.
4. Click **Save**, and then apply your **Pending changes**.

△ | **CAUTION: Your appliance will be rebooted to apply these changes. Any connections will be terminated.**

Zeroization

Zeroization is the practice of permanently destroying all critical security parameters. This is accomplished by overwriting the entire disk with zeros. Zeroization makes it very hard to retrieve sensitive data from the appliance. It is used before recycling hardware, or in other cases where data security is more important than retaining the data. After this operation is completed, the appliance can no longer be used at your site and must be returned to SonicWall for replacement hardware to restore service.

To zeroize the appliance:

1. In the AMC, navigate to **System Configuration > Maintenance**.
2. Select **Reset**.
3. On the **Reset** page, select the type of reset you want to perform as explained in Resetting the Appliance.
4. When the reset begins, stay physically present with the appliance until the appliance halts.

   △ | **CAUTION: Your appliance can take up to 45 minutes to complete the zeroization process.**

Software Licenses

This section describes how to manage software licenses for appliance components. The SMA appliance uses different types of licenses:

- **Administration test license**: When you receive your SMA appliance, you must log in to MySonicWall to retrieve your initial user license, which is valid for one user (the administrator plus one end user) for an unlimited number of days. This allows you to become familiar with the AMC, which you will use to upload an appliance license file for additional users or other components.
- **Appliance licenses**: This license is used to monitor and enforce concurrent user counts. If you exceed your concurrent active user limit, user access is restricted until the active user count drops below the licensed user limit.

  Concurrent user support by SMA appliances is shown in the below table:

Concurrent User Support By SMA Appliance

SMA appliance	Supports concurrent users up to
SMA-8200v	5000
SMA-7200	10000
SMA-7210	10000
SMA-6200	2000
SMA-6200	2000

If user access is restricted, users attempting to log in to your VPN see an error message indicating that the license count may have been exceeded, and they are denied access to your network.

- **Component licenses**: If the license for an appliance component has expired, users attempting to use that component see an error message in WorkPlace. In the case of a Spike License, the number of days remaining on it and how many users are covered by it are displayed in AMC.
- **Pooled licenses**: The pooled licensing model allows central user licenses to be shared among the managed appliances so that central user licensing is resilient to the failure of (or communication loss with) the CMS or any one appliance. For more information, see “Central User Licensing” in the *SMA CMS Administration Guide*.

All appliance license files must be retrieved from www.mysonicwall.com and imported to the appliance, as described in Managing Licenses.

ⓘ **NOTE:** Central Management Server (CMS) licenses should not be manually imported. For proper operation, the CMS must retrieve its license from MySonicWall when you register your CMS. For more information, refer to the *SMA CMS Administration Guide*.

Topics:

- How Licenses Are Calculated
- Viewing License Details
- Managing Licenses

How Licenses Are Calculated

A user license for the appliance does not represent a person, but rather a user authentication. If a user logs in to WorkPlace on a desktop computer, for example, and is also logged in on a mobile device, two licenses are consumed as soon as the user accesses a resource that’s protected by the appliance.

A license is released when a connection has been inactive for 15 minutes. How this inactivity is measured depends on the user’s access method:

- With translated, custom port mapped, or custom FQDN mapped Web access, the license is released after 15 minutes during which no resources are accessed.
- When Connect Tunnel is running, the connection to the appliance is kept open, which means that the license is in use as long as the tunnel is up. Once the tunnel is disconnected, the license is released after 15 minutes.

There are a few ways to restrict or end sessions:

- Restrict the number of licenses that a person can have on a per-community basis. When the limit is reached, no further appliance sessions (and no access to resources) are allowed. The user can start a new session only by terminating existing sessions. For a description of the **Maximum active sessions** setting, see Assigning Members to a Community.
- Have tunnel client sessions terminate-on a per-community basis-when the time period set for **Credential lifetime** (on the **Configure General Appliance Options** page) is reached, where the **Limit session length to credential lifetime** setting is enabled by default. See Ending User Sessions.
- Terminate a user session manually. See Viewing User Sessions for information on how to end user sessions in AMC. Also see Open vs Licensed Sessions for more on the distinction between different types of sessions.

ⓘ **NOTE:** Users who reach the limit of their appliance licenses and then attempt to authenticate with just a client certificate are not prompted to terminate all existing sessions. These users must terminate an existing session in order to free up a license and start a new one. The best method for terminating a session is for the user to log out, otherwise he or she must wait 15 minutes for the session to time out and a license to be released.

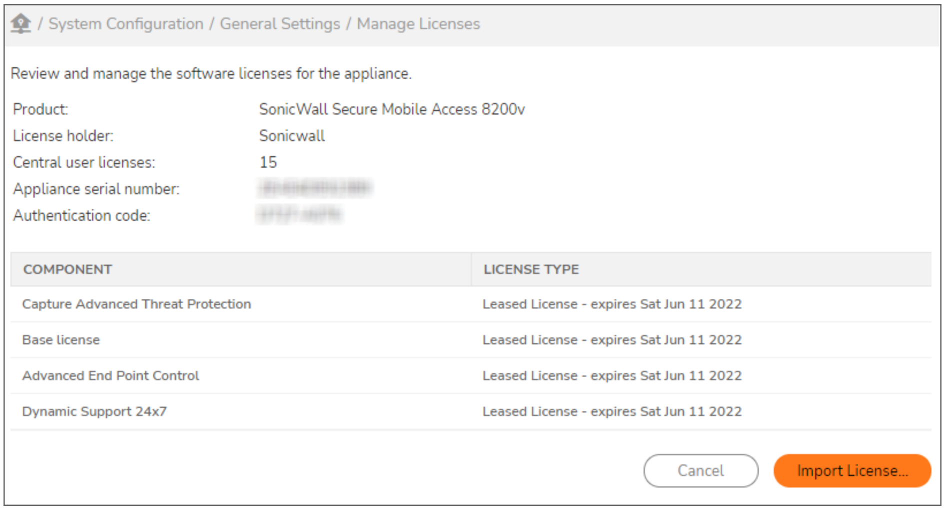
Viewing License Details

In AMC, you can view the status of your base appliance license and the licenses for any other appliance components you may have purchased, such as OnDemand or Spike License. This section describes how to view details about the status of your licenses.

To view license details:

1. In the AMC, navigate to **System Configuration > General Settings**.
2. Click the **Edit** link in the **Licensing** section.

   The **Manage Licenses page** displays.



/ System Configuration / General Settings / Manage Licenses

Review and manage the software licenses for the appliance.

Product:	SonicWall Secure Mobile Access 8200v
License holder:	Sonicwall
Central user licenses:	15
Appliance serial number:	[redacted]
Authentication code:	[redacted]

COMPONENT	LICENSE TYPE
Capture Advanced Threat Protection	Leased License - expires Sat Jun 11 2022
Base license	Leased License - expires Sat Jun 11 2022
Advanced End Point Control	Leased License - expires Sat Jun 11 2022
Dynamic Support 24x7	Leased License - expires Sat Jun 11 2022

3. Review the information provided, as shown in the below table:

License Information

License information	Description
Product	The type of SMA appliance to which the license applies.
License holder	The name of the entity to whom the appliance is licensed.
Maximum concurrent users	The maximum number of concurrent user sessions allowed by the base appliance license. A concurrent user is a single login from a single IP address. Users are not counted once they log off, or when their credentials expire. If a Spike License is in effect, you'll see the total number of allowed users, the number of days remaining for the license, and at what time the next day begins. For example: `Spike license: 100 users, 60 days Active: Currently on day 2 of 60. Day 3 will begin at 10:15 PM on 9/23/09.` You can pause the Spike License as needed; see Managing a Spike License for more information.
Appliance serial number	The serial number is burned into the firmware on hardware appliances. Only on virtual is it derived from the license file.

Authentication code	This is the appliance hardware identifier. The license you obtain from www.mysonicwall.com will be valid only for the appliance with this authentication code. See Managing Licenses for information on obtaining your license file.
Component and license type	Details about any individual software component licenses. If the license is a temporary or evaluation license, the expiration date is displayed. If a license expiration date is approaching, or if a license has expired, a warning message is displayed in this area and in the AMC status area.

Managing Licenses

This section describes how to obtain your appliance licenses from www.mysonicwall.com. You must have a base appliance license file if, for example, you want to replace an evaluation license with a permanent license after deciding to purchase an appliance. There are also some components—such as Connect and Spike License—that require a separate purchase and license.

ⓘ **NOTE:** Central Management Server (CMS) licenses should not be manually imported. For proper operation, the CMS must retrieve its license from MySonicWall when you register your CMS. For more information, refer to the *SMA CMS Administration Guide*.

Before you can enable your appliance or a component that requires a separate purchase and license, you must follow these steps:

1. Create a MySonicWall account, if you don't already have one. You need an account to register your appliance. (MySonicWall registration information is not sold or shared with any other company.) See Creating a MySonicWall Account for more information.
2. Register your device on MySonicWall. Registration provides access to essential resources, such as your license file, firmware updates, and technical support information. See Registering Your SMA Appliance for more information.
3. Use your MySonicWall account to apply the license for your appliance.
4. Apply your license file in AMC; see Downloading and applying SMA license for more information.

△ **CAUTION: You should ensure that the appliance's date and time settings are configured correctly for your time zone before importing a license file. For information about configuring the system clock settings, see Configuring Time Settings.**

Topics:

- Creating a MySonicWall Account
- Registering Your SMA Appliance
- Downloading and applying SMA license
- Managing a Spike License

Creating a MySonicWall Account

To create a MySonicWall account, complete the short online registration form. Registration information is not sold or shared with any other company.

To create a MySonicWall account:

1. In your Web browser, go to the MySonicWall Web site: https://www.mysonicwall.com/.
2. In the **User Login** section, follow the link for unregistered users.
3. Enter your account information, personal information, and preferences, and then click **Submit**.

   Be sure to use a valid email address.
4. Follow the prompts to finish creating your account. SonicWall will send a subscription code to the email address you entered in *Step 3*.
5. When you return to the login screen, log in with your new username and password.
6. Confirm your account by entering the subscription code you received in email.

Registering Your SMA Appliance

Registration provides access to essential resources, such as your license file, firmware updates, documentation, and technical support information.

To log in to your MySonicWall account and register your appliance:

1. In your Web browser, go to the MySonicWall Web site and log in with your username and password: https://www.mysonicwall.com/
2. Locate your software **Serial Number**, which is printed on the back of your SMA appliance.

   ⓘ **NOTE:** For virtual appliance , once you provision the product in MySonicWall, the serial number is generated. For more information, refer to Downloading and applying SMA license.
3. Enter your serial number, and then click **Next**. Follow the on-screen instructions.
4. Confirm your **Serial Number**.
5. Enter a name for this appliance.
6. Enter the authentication code for this appliance, which is the hardware identifier for the appliance you purchased. The authentication code is displayed in AMC: click **General Settings** from the main navigation menu, and then look in the **Licensing** area.

   For virtual serial number, the authentication code is empty by default.
7. Click **Register** to continue.

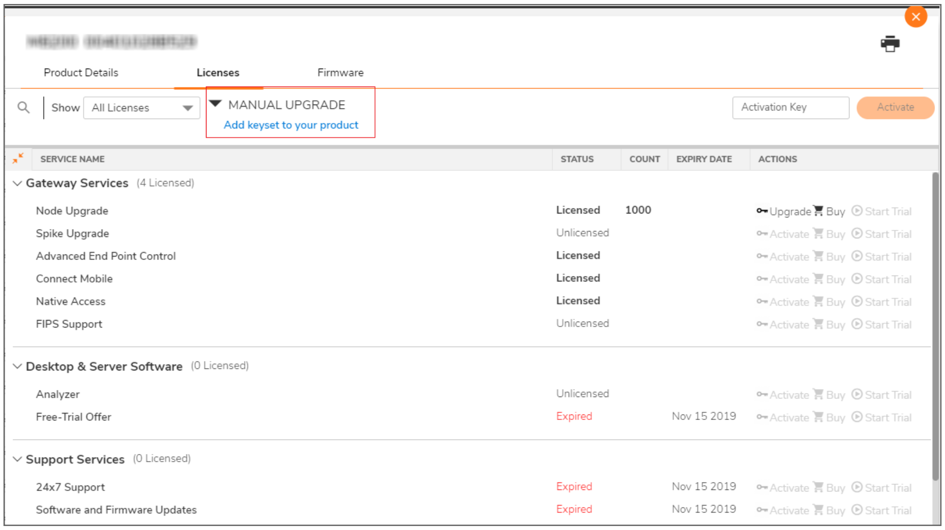
Follow the online prompts to fill out the survey and complete the registration process.

Downloading and applying SMA license

The SMA appliance ships with a single administration test license that supports one user indefinitely; to test or deploy the appliance with additional users, or to enable separate components, such as a Spike License, you must apply a valid license file.

To download the license file from MySonicWall and import it:

1. In your Web browser, go to the MySonicWall Web site and log in with your username and password: https://www.mysonicwall.com/
2. Go to **My Products**.
3. Click the link for the appliance that requires a license.
4. Click on the **Licenses** tab.

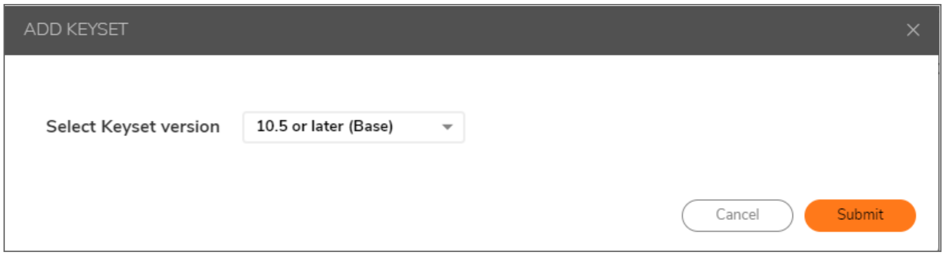


[redacted]

SERVICE NAME	STATUS	COUNT	EXPIRY DATE	ACTIONS
Gateway Services (4 Licensed)				
Node Upgrade	Licensed	1000		Upgrade Buy Start Trial
Spike Upgrade	Unlicensed			Activate Buy Start Trial
Advanced End Point Control	Licensed			Activate Buy Start Trial
Connect Mobile	Licensed			Activate Buy Start Trial
Native Access	Licensed			Activate Buy Start Trial
FIPS Support	Unlicensed			Activate Buy Start Trial
Desktop & Server Software (0 Licensed)				
Analyzer	Unlicensed			Activate Buy Start Trial
Free-Trial Offer	Expired		Nov 15 2019	Activate Buy Start Trial
Support Services (0 Licensed)				
24x7 Support	Expired		Nov 15 2019	Activate Buy Start Trial
Software and Firmware Updates	Expired		Nov 15 2019	Activate Buy Start Trial

5. Under the **MANUAL UPGRADE** click **Add keyset to your product**.

   The **Add Keyset** page is displayed.



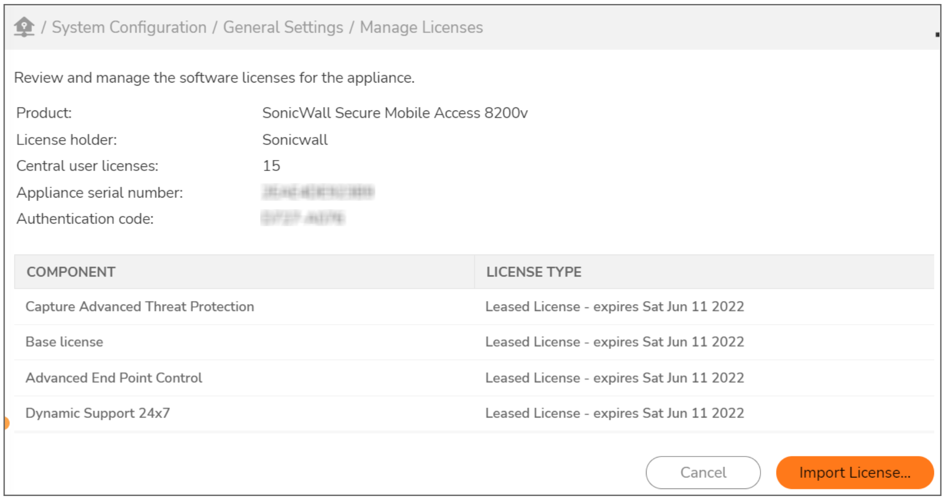
ADD KEYSET

Select Keyset version: 10.5 or later (Base)

6. Select the version to download the license file and click **Submit**.

   The license file (`.lic`) is downloaded in your device.
7. In the AMC, navigate to **System Configuration > General Settings**.
8. In the **Licensing** section, click **Edit**.

   ⓘ **NOTE:** Based on the license type purchased and the applications that you use, you may see different license type description. For example, SMA1000 CMS with central user license type displays **Leased License** in the license type description. However, the functionality of the appliance remains the same.
9. Click **Import License**.



Review and manage the software licenses for the appliance.

Product:	SonicWall Secure Mobile Access 8200v
License holder:	Sonicwall
Central user licenses:	15
Appliance serial number:	[redacted]
Authentication code:	[redacted]

COMPONENT	LICENSE TYPE
Capture Advanced Threat Protection	Leased License - expires Sat Jun 11 2022
Base license	Leased License - expires Sat Jun 11 2022
Advanced End Point Control	Leased License - expires Sat Jun 11 2022
Dynamic Support 24x7	Leased License - expires Sat Jun 11 2022

10. In the **License File Upload** click **Choose File** and select the downloaded license file.
11. Click **Upload**.
12. Click **Save** and apply pending changes.

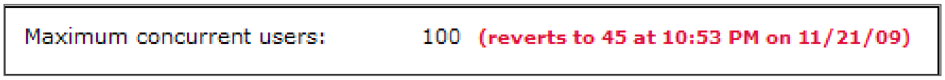
Managing a Spike License

A Spike License enables you to temporarily increase the number of remote users you can support in the event of a disaster or other business disruption. Licensed separately, this feature helps you accommodate spikes in remote access traffic during planned or unplanned events.

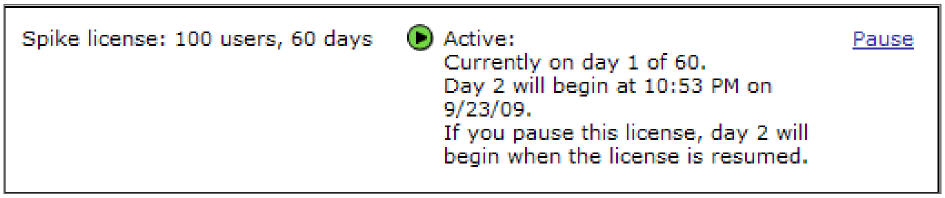
When you buy a Spike License it is valid for a given number of users and days (this is the total number of users who are supported when the Spike License is activated, not in addition to your base license number). You can suspend and resume the use of the license as needed.

To activate, pause, and resume a Spike License:

1. Retrieve your Spike License from MySonicWall and import it to the appliance, as described in Downloading and applying SMA license.
2. The Spike License is listed as **Available** on the **Manage Licenses** page in AMC. When you need to accommodate more users, click **Activate**. The maximum number of possible users is updated, and the time line for your Spike License is displayed.



Maximum concurrent users: 100 (reverts to 45 at 10:53 PM on 11/21/09)



Spike license: 100 users, 60 days

Active:
Currently on day 1 of 60.
Day 2 will begin at 10:53 PM on 9/23/09.
If you pause this license, day 2 will begin when the license is resumed.

3. Click **Pause** to suspend use of the Spike License, and click **Resume** to continue using it.

ⓘ | **NOTE:**

- You can upload more than one Spike License to your appliance, but you cannot have more than one active at a time.
- Whenever you activate or pause a Spike License, the number of days for which it is valid decreases by one, even if fewer than 24 hours have elapsed.

Using Global Overrides

Global overrides are recommended to be used only during troubleshooting. The main aim of global overrides is to provide the ability to easily override community-specific settings to make it easier to troubleshoot the issues.

Use global overrides to override the following community settings:

- ESP Mode
- Software Updates
- Limit session length to credential lifetime

  ⓘ | **NOTE:** Changes made from Global overrides cannot be seen in AMC Community UI but are applied on policy level.

Topics:

- Configuring Global Overrides in AMC

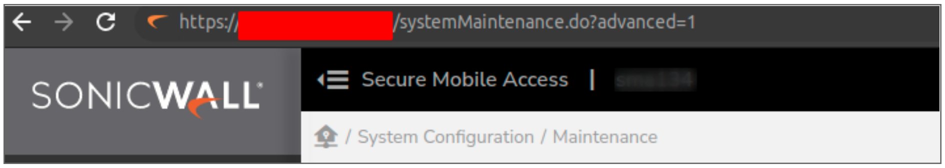
Configuring Global Overrides in AMC

Prerequisites:

- SMA/CMS running 12.4.2 firmware versios.

To configure global overrides in AMC:

1. In the AMC, navigate to **System Configuration** > **Maintenance**.
2. Append **?advanced=1** in the URL.

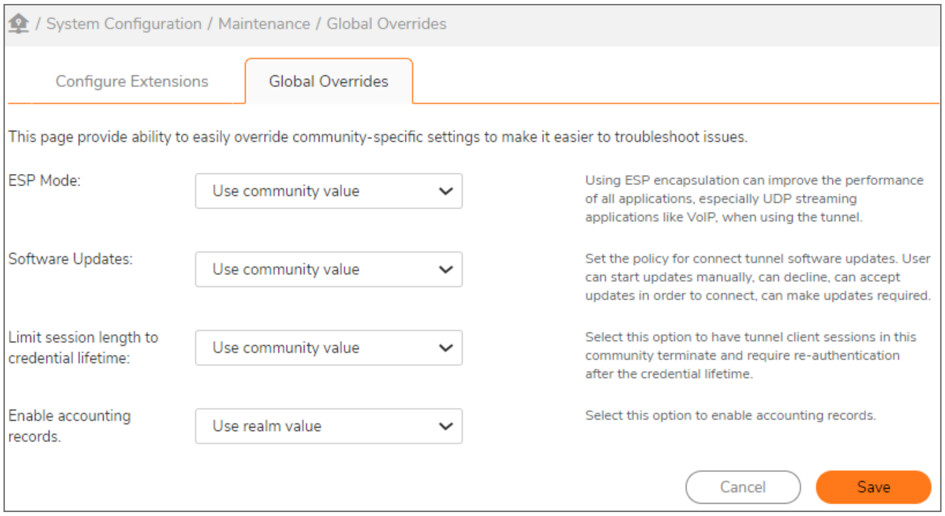


https://[redacted]/systemMaintenance.do?advanced=1

SONICWALL
Secure Mobile Access | [redacted]
/ System Configuration / Maintenance

The **Advanced** section with **Configuration Extensions** and **Apply All** options are displayed.

3. Under **Configuration Extensions**, click **Configure**.
4. Click the **Global Overrides** tab.



This page provide ability to easily override community-specific settings to make it easier to troubleshoot issues.

ESP Mode:	Use community value	Using ESP encapsulation can improve the performance of all applications, especially UDP streaming applications like VoIP, when using the tunnel.
Software Updates:	Use community value	Set the policy for connect tunnel software updates. User can start updates manually, can decline, can accept updates in order to connect, can make updates required.
Limit session length to credential lifetime:	Use community value	Select this option to have tunnel client sessions in this community terminate and require re-authentication after the credential lifetime.
Enable accounting records.	Use realm value	Select this option to enable accounting records.

5. Configure the following settings:

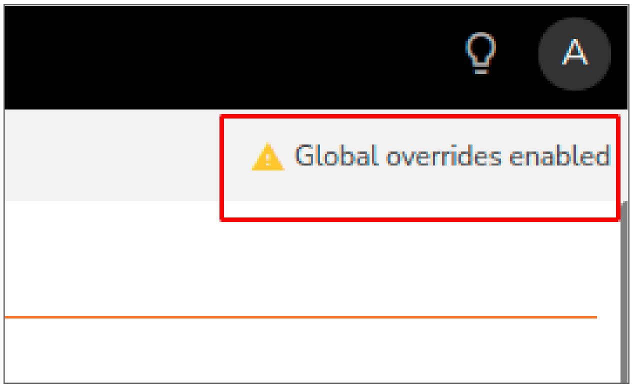
Settings	Descriptions
ESP Mode	To troubleshoot if some service or application or resource is not working. • Do not use ESP mode • Use for all network traffic • Use for UDP traffic only • Use realm value To leave the community-specific settings intact, select the **Use community value** option.

Settings	Descriptions
Software Updates	To set the policy for connect tunnel software updates. • Manual • At Users discretion • Required • Forced • Use realm value To leave the community-specific settings intact, select the **Use community value** option.
Limit Session length to credential lifetime	• True: To terminate the tunnel client sessions in this community and require to re-authenticate after the same length of time. • False: To keep the established Connect Tunnel session active and never terminated by the appliance. To leave the community-specific settings intact, select the **Use community value** option.
Enable accounting records	• True: To enable accounting records, irrespective of what is set at individual realm level. • False: To disable accounting records for all the realms, irrespective of what is set at individual realm level. To leave the realm-specific settings intact, select the **Use realm value** option.

6. Click **Save** and apply pending changes.

   AMC displays a message bar warning on top right when any global overrides are in effect.

   Clicking on the warning takes the admin directly to the overrides page.



ⓘ | **NOTE:** Some important notes on the Global Overrides settings:

- If the global variable is configured or in use, then you can access the **Global Override** settings directly clicking the **Global overrides enabled** warning message. Note that you need not add any special URL.

6

End Point Control

Topics:

About End Point Control

The SMA appliance includes support for End Point Control, which you can use to protect sensitive data and ensure that your network is not compromised when accessed from devices in untrusted environments. End Point Control works by:

- Verifying that the user's environment is secure
- Controlling access to sensitive resources

Traditional VPN solutions provide access only from the relative safety of a corporate laptop. In that environment, one of the biggest security concerns is unauthorized network access. An SSL VPN, on the other hand, enables access from any Web-enabled system, including devices in untrusted environments. A kiosk at an airport or hotel, or an employee-owned computer, increases the risk to your network resources.

End Point Control reduces your exposure from untrusted environments in three ways:

- **Verifying that the user's environment is secure** – Corporate IT departments configure computers under their control with antimalware software, firewalls, and other safeguards designed to protect them from malicious software (malware). In contrast, unmanaged computers can easily contain keystroke recorders, viruses, Trojan horses, and other hazards that can compromise your network.

  Secure Mobile Access lets you define zones of trust that provide different levels of access depending on the level of trust at the user's end point. Connection requests are compared against device profiles you set up in AMC and then assigned to the appropriate zone.
- **Controlling access to sensitive resources** – You can reference End Point Control zones in access control rules. For example, a connection originating from a less trusted EPC zone can be denied access to sensitive resources.

End Point Control and OESIS

The OESIS framework is a cross-platform software development kit used within Secure Mobile Access to help secure and manage endpoints connected to the infrastructure. For Secure Mobile Access 12.4, the OESIS framework was upgraded to Version 4, which allows for faster execution of code, more frequent updates and the ability for out-of-the-band definition updates. Customers having versions 11.4.x and 12.0.x should update to 12.4 to get the full advantage of these benefits.

All newly created profiles will be OESIS V4 compliant, but if you upgraded from a prior version, it is recommended that you delete the existing profiles and recreate them so they will be V4 complaint as well. In OESIS V4, a new category, **Anti-Malware Program**, has been developed. It replaces the Anti-Virus Program and the Anti-Spyware Program since many products qualify in both categories these days.

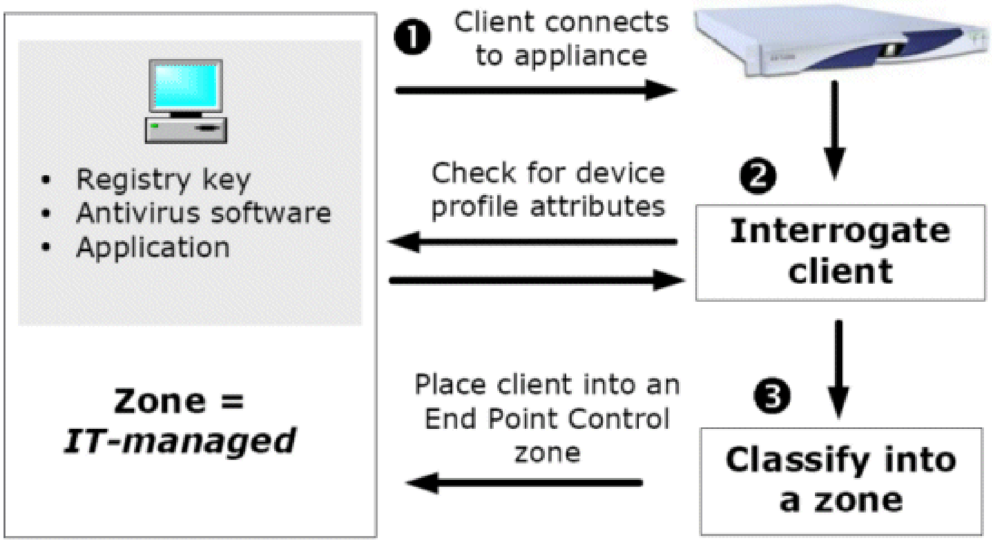
ⓘ | **NOTE:** The OESIS V3 libraries have already been declared out of support by OPSWAT.

- If you have OPSWAT V3 attributes configured, upgrading to SMA 12.4 fails. To overcome this scenario, remove the OPSWAT V3 attributes and proceed the upgrade process.
- Importing old configuration with OPSWAT V3 attributes/profiles would block applying “Pending Changes” until those are deleted.

How the Appliance Uses Zones and Device Profiles for End Point Control

End Point Control is managed and deployed at the community level on the appliance. An authentication realm-the entry point to the appliance for users contains one or more communities, which are collections of users or groups with similar access needs. A community in turn use one or more EPC zones. EPC zones can reference one or more device profiles, which define the attributes that must be present on a client computer. The EPC process works this way:

End Point Control For Zone IT-Managed



Registry key
Antivirus software
Application
Zone =
IT-managed
❶ Client connects to appliance
Check for device profile attributes
❷
Interrogate client
Place client into an End Point Control zone
❸
Classify into a zone

1. A user connects to the appliance:
   a. The user logs in to an authentication realm.
   b. The appliance assigns the user to a community that belongs to that realm.
2. The appliance interrogates the user’s computer to determine if it has attributes (contained in a device profile) that match those defined in one of the community’s EPC zones.
3. If the device matches a profile, the appliance classifies the device into a particular EPC zone and deploys the EPC tools configured for that zone.
4. If the user is connecting with a personal device, they may optionally be prompted to authorize the VPN connection.

In this case, the user’s device profile matches an End Point Control zone named *IT-managed*. For a more detailed description of this process, see Scenario 1: Employees Connecting from IT-Managed Laptops.

ⓘ | **NOTE:**

- During client interrogation, the device profile attributes that the appliance is checking for and whether they were found is recorded in the system message log, provided the log level is set to verbose. See End Point Control Interrogation for more information.

Defining Zones

There are three categories of zones that you can customize, plus a built-in zone (**Default**); see the below table. A community can include **Deny**, **Device**, and **Quarantine** zones; the **Default** zone, on the other hand, is global. See Adding Communities to a Realm for more information about communities.

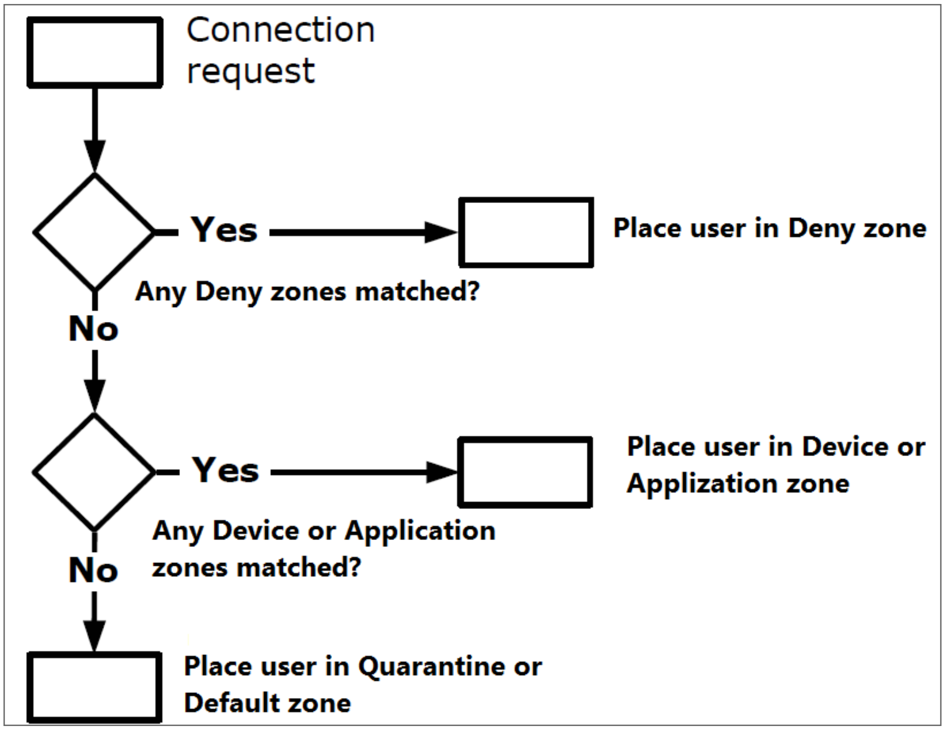
Types Of Zones

Zone type	Description

Deny	Deny zones are evaluated first. The appliance tries to find a match in the list of **Deny** zones, starting with the one at the top. If there is a device profile match (for example, a certain file is found on the device), the user is denied access to the network. See Creating a Deny Zone for more information.
Device	If the device does not match the criteria for a **Deny** zone, the appliance tries to find a match in the list of Standard zones, starting with the one at the top. The standard zone category contains the **Device** zone. If the device matches the criteria, it is placed in a zone of trust. If no match is found, the device is placed in the **Default** zone or in a **Quarantine** zone (if one is defined). See Creating a Device Zone for more information.
Quarantine	A device for which there is no profile match is placed in either the Default zone or in a Quarantine zone. You can customize the message users see; for example, you may want to explain what is required to bring the user's system into compliance with your security policies. There can be only one Quarantine zone in a community. See Creating a Quarantine Zone for more information.
Default	This zone is global and implicitly present in every community configured in AMC. If a device does not match any other profile, you choose whether it should "fall through" to the Default zone or to a Quarantine zone. You can customize the Default zone to some extent, but you cannot delete it. See Configuring the Default Zone for more information.

The below image illustrates the order in which zones are evaluated. Only the **Default** zone is required:

Zone Evaluation Order


Connection request
Yes
Place user in Deny zone
Any Deny zones matched?
No
Yes
Place user in Device or Applization zone
Any Device or Application zones matched?
No
Place user in Quarantine or Default zone

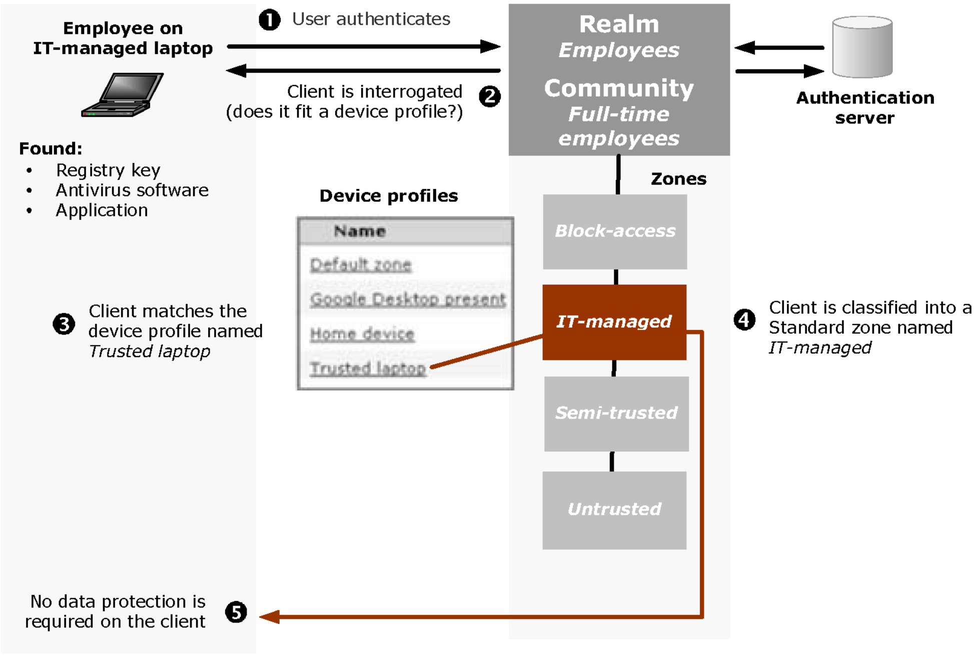
End Point Control Scenarios

This section describes some typical End Point Control scenarios that use zones and device profiles to classify connection requests and deploy End Point Control tools to clients.

Topics:

- Scenario 1: Employees Connecting from IT-Managed Laptops
- Scenario 2: Employees Connecting from a Home PC
- Scenario 3: Employees Connecting from a Public Kiosk
- Scenario 4: Employee Connects from a PC with Google Desktop
- Scenario 5: Employee Connects from a Mobile Device

Scenario 1: Employees Connecting from IT-Managed Laptops

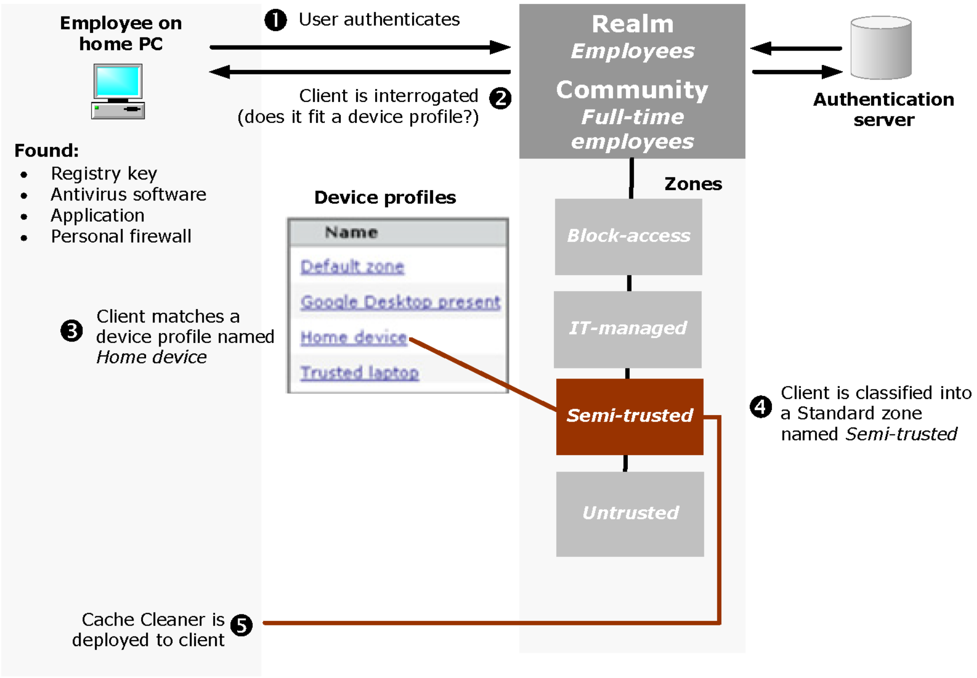


This scenario begins with an employee connecting to the appliance using an IT-managed laptop:

1. The user connects to the appliance, logs in to the realm *Employees*, and is assigned to the *Full-time employees* community.
2. After the user authenticates, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the *Full-time employees* community. Device profiles are evaluated by zone, starting with any Deny zones and then proceeding through the zones listed for the community.

3. The appliance finds that the client doesn't match the device profile for the **Deny** zone (*Block-access*), so it proceeds to check the profile for the *IT-managed* zone. The *IT-managed* zone references a device profile named *Trusted laptop*. The appliance determines that the user's device attributes match that particular device profile (a registry key entry, antimalware software, and an application).
4. Based on that match, the appliance classifies the device into the *IT-managed* zone and doesn't evaluate the subsequent zones in the list for that community.
5. The *IT-managed* zone is not configured to require a data protection tool on the client. The appliance then provisions the access agent configured for the *Full-time employees* community, and the user is able to access the appropriate network resources.

Scenario 2: Employees Connecting from a Home PC



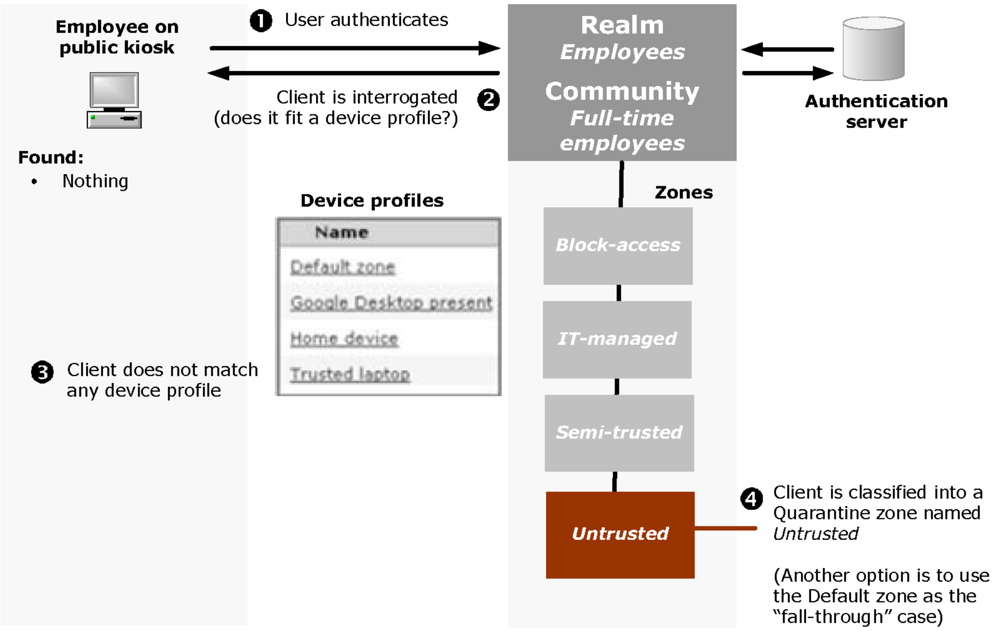
This scenario begins with an employee connecting to the appliance from a home PC:

NOTE: From 12.4.2 onwards, Cache Cleaner functionality is no longer supported in Mac or Windows platforms.

1. The user connects to the appliance, logs in to the realm *Employees*, and is assigned to the *Full-time employees* community.
2. Once the user is authenticated, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the *Full-time employees* community. Device profiles are evaluated by zone, starting with any Deny zones and then proceeding through the others listed for the community.

3. In this scenario, the appliance finds that the client doesn't match the device profile for the Deny zone (*Block-access*) or the Standard zone named *IT-managed*, so it continues to the next one in the list: *Semi-Trusted*.
4. The *Semi-trusted* zone references a device profile named *Home device*. The appliance determines that the user's device attributes (a registry key entry, antimalware software, an application, and a personal firewall) match that device profile.
5. Based on that match, the appliance classifies the device into the *Semi-trusted* zone and doesn't evaluate the subsequent zones in the community.
6. Because the *Semi-trusted* zone is configured to require a data protection tool on the client, the appliance deploys Cache Cleaner to the client. The appliance then provisions the access agent configured for the *Full-time employees* community, and the user is able to access the appropriate network resources.

Scenario 3: Employees Connecting from a Public Kiosk



This scenario begins with an employee connecting to the appliance from a public kiosk:

ⓘ **NOTE:** From 12.4.2 onwards, Cache Cleaner functionality is no longer supported in mac or windows platforms.

1. The user connects to the appliance, logs in to the realm *Employees*, and is assigned to the *Full-time employees* community.
2. After the user authenticates, the client device is interrogated to determine if it matches any device profiles belonging to zones referenced by the *Full-time employees* community, starting with any Deny zones and proceeding through the others listed for the community.
3. In this scenario, the appliance finds that the client doesn't match any of the configured device profiles. There are a couple of ways to handle this sort situation: classify the client into a **Quarantine** zone, or into

the **Default** zone. In this example, the **Quarantine** zone *Untrusted* is used. The only resources a user has access to are those that you have set up: you might, for example, display a customized page with links to Web resources for bringing a system into compliance with your security policies.

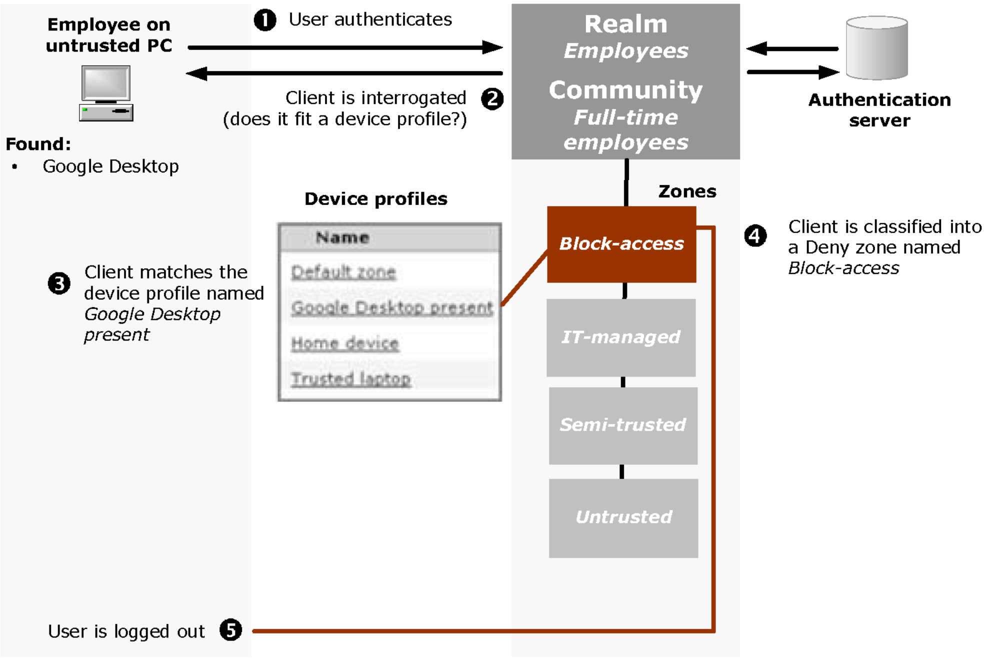
a. If the untrusted device (for example, a PC in a public kiosk) is running Windows 10, Windows Vista, or Windows 2008 Server, and a supported browser, the user is required to download and install the client component manager, Secure Endpoint Manager. The client component manager automatically deploys Cache Cleaner for the user. The appliance then provisions the access agent configured for the *Full-time employees* community, and the user can access the appropriate network resources.

b. If the device's operating system and browser are not compatible with Cache Cleaner, a message is displayed.

c. If Cache Cleaner cannot be deployed on the client, the user's connection request is denied.

See Configuring the Default Zone for information on the setup options for this zone.

Scenario 4: Employee Connects from a PC with Google Desktop



An employee connects to the appliance from a PC outside of the corporate office:

1. The user connects to the appliance, logs in to the realm *Employees*, and is assigned to the *Full-time employees* community.
2. After the user authenticates, the client device is interrogated to determine if it matches any device profiles belonging to the zones referenced by the *Full-time employees* community, starting with any Deny zones.
3. In this case the appliance determines that the PC is running Google Desktop, which makes it a match for the Google Desktop present device profile. The device is classified into the Deny zone named *Block-*

access.

4. No other zones are evaluated and the user's access request is denied.
5. The user is logged out.

Scenario 5: Employee Connects from a Mobile Device

In this scenario an employee connects to the appliance from a mobile device outside of the corporate office. To establish an association between a particular user and his or her device (in case the device is misplaced or lost), the administrator has collected the user name and IMEI (International Mobile Equipment Identity) number for each device, and has added the IMEI number for user accounts on the Active Directory server. The administrator has also created a device profile named *Mobile resources* that verifies that user/IMEI association.

When a user logs in, the sequence is:

1. The user connects to the appliance, logs in to the realm *Employees* by entering a user name and password, and is then assigned to the *Mobile employees* community.
2. After the user authenticates, the client device is interrogated (using a device profile for the zone referenced by the *Mobile employees* community) and its IMEI number is determined.
3. The IMEI number is compared against the one that is associated with the user in the AD directory. If there's a match, the user is allowed access to mobile device-specific links; otherwise he or she is denied access.
4. Optionally, the user may be prompted to authorize the VPN connection from the personal device.

ⓘ **NOTE:** Checking for an IMEI number works only on wide area networks (WAN), not WiFi, and the WAN service must be on for the post-authentication process to determine the IMEI number on the mobile device.

To track service by mobile device and user you can process audit log files for network proxy, Web proxy, or tunnel clients.

Managing EPC with Zones and Device Profiles

Device profiles can include any combination of the following attributes to identify a client and assign it to a "zone of trust," quarantine it, or deny it access altogether:

- Application
- Client certificate
- Directory name
- Equipment ID (the identifier for a device; for example, the IMEI number of a mobile device)
- File name, size, or timestamp
- Windows domain
- Windows registry entry

- Windows version
- Microsoft Intune

If you are licensed for Advanced EPC, you have additional attributes for identifying security programs on client devices:

- Antimalware program
- Personal firewall program

And, you can define fallback detection for these types of security programs using the EPC library. See Advanced EPC: Using Fallback Detection for configuration instructions.

An EPC zone can reference use one or more device profiles. Multiple device profiles are useful if there are users with similar VPN access needs who use different computer platforms. For example, you could configure an EPC zone that references a device profile for Windows computers, and another zone for MacOS computers. AMC supports device profiles for Windows, MacOS, Linux, and other mobile devices (such as PDAs and smart phones). You can create multiple zones and device profiles as needed to accommodate different access scenarios and levels of trust, such as separate zones for employees, business partners, or contractors.

AMC includes a predefined zone and some device profiles:

- You can customize the **Default** zone to some extent, but you cannot delete it. A device that cannot be classified into any of the zones you have configured is placed in either the **Default** zone, or a **Quarantine** zone. (When you configure a community, you choose which of these will be the fallback zone; see Using End Point Control Restrictions in a Community for how to do this.) See Configuring the Default Zone for more information.
- To help you get started with Advanced EPC, the appliance includes some preconfigured device profiles designed for common access scenarios. You can use these as is, or customize them to meet your needs; see Advanced EPC: Using Preconfigured Device Profiles for more information.

Communities are used to specify which zones are available to users after they authenticate. For information on linking zones to communities, see Using End Point Control Restrictions in a Community. In addition, you can tie zones to your access policy in much the same way as users, groups, and resources.

Topics:

- Enabling and Disabling End Point Control
- Configuring and Using Zones and Device Profiles
- Creating Zones for Special Situations
- Using End Point Control Agents

Enabling and Disabling End Point Control

You can globally enable or disable End Point Control in AMC.

When End Point Control is disabled (which is the default setting), the appliance does not perform the following EPC actions:

- Evaluate the attributes of client devices
- Classify connection requests into zones
- Enforce zone restrictions in access control rules

ⓘ **NOTE:** If End Point Control is disabled, settings for the Default Zone are applied to all user sessions because, with End Point Control disabled, all users are put in the Default Zone.

To enable End Point Control:

1. In the AMC, navigate to **User Access > End Point Control**.
2. In the **General** section, click **Edit.**

   The **End Point Control Settings** page displays.
3. Select **Enable End Point Control**.
4. Click **Save.**

ⓘ **NOTE:** When EPC is enabled, you can specify (on a per-zone basis) how often EPC checks are done: only once (at login), or at login and then every *<n>* minutes for the duration of the session. See Creating a Device Zone or Configuring the Default Zone for more information.

Configuring and Using Zones and Device Profiles

Topics:

Viewing Zones

You can see the list of End Point Control zones in AMC and quickly determine what types they are and whether there are any communities associated with them.

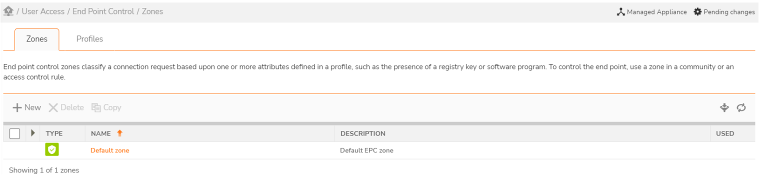
To view configured zones:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.

3. The **Zones and Profiles page** displays to provide a summary of the zones configured in AMC and a summary of the EPC agent status. The SMA appliance comes with a preconfigured zone named **Default zone**.

   End point control zones classify a connection request based upon one or more attributes defined in a profile, such as the presence of a registry key or software program. To control the end point, use a zone in a community or an access control rule.

□	TYPE	NAME	DESCRIPTION	USED
	✓	Default zone	Default EPC zone	

   Showing 1 of 1 zones

   You can see information about each zone in the list:

   - Expand a selected zone to display the device profiles and communities the zone is associated with. Clicking the plus sign in the table header expands the display of every zone.
   - The **Type** column identifies whether a given zone is a **Default**, **Device**, **Deny**, or **Quarantine** one (these zone types are described in detail in Defining Zones).
   - The **Name** column displays the name you assigned when creating a zone; edit a zone by clicking its name.
   - The **Description** column lists any descriptive text for the zone.
   - The **Used** column indicates whether the zone is used by any communities. A tick mark indicates it is being used by one or more communities. If a zone is not referenced, this field is blank.

4. Click the name of a zone to view or edit its settings.

Viewing Device Profiles

Device profiles specify the attributes used to identify a client, such as the presence of a registry key or software program. They are used by End Point Control zones.

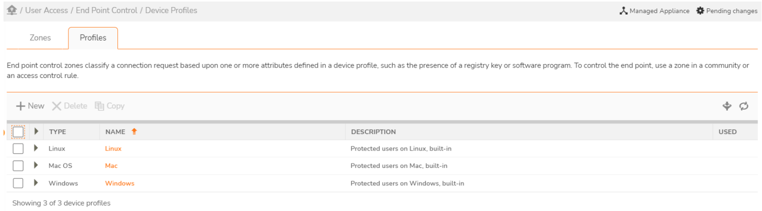
To view configured device profiles:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.

   The **Zones and Profiles** page displays.



End point control zones classify a connection request based upon one or more attributes defined in a device profile, such as the presence of a registry key or software program. To control the end point, use a zone in a community or an access control rule.

TYPE	NAME	DESCRIPTION	USED
Linux	Linux	Protected users on Linux, built-in	
Mac OS	Mac	Protected users on Mac, built-in	
Windows	Windows	Protected users on Windows, built-in	

Showing 3 of 3 device profiles

- The **Name** column displays the name you assigned when creating the device profile; edit a device profile by clicking its name.
- The **Description** column lists any descriptive text for the device profile.
- The **Type** column displays the device profile platform names: **Microsoft Windows**, **macOS**, **Linux**, and **Other mobile device**.
- The **Used** column indicates whether the profile is used by any clients. A tick mark indicates it is being used by one or more Zones. If profile is not used, this field is blank.

3. In the **Device Profiles** section, review the list of configured profiles. If you have Advanced EPC, this list includes several preconfigured device profiles.

Creating a Device Zone

Device zones are evaluated after **Deny** zones. You could create a device profile, for example, named *Windows firewall* that would require that a personal firewall be running. When this End Point Control policy is in place, any device that is a match is placed in a zone of trust.

To define a Device zone:

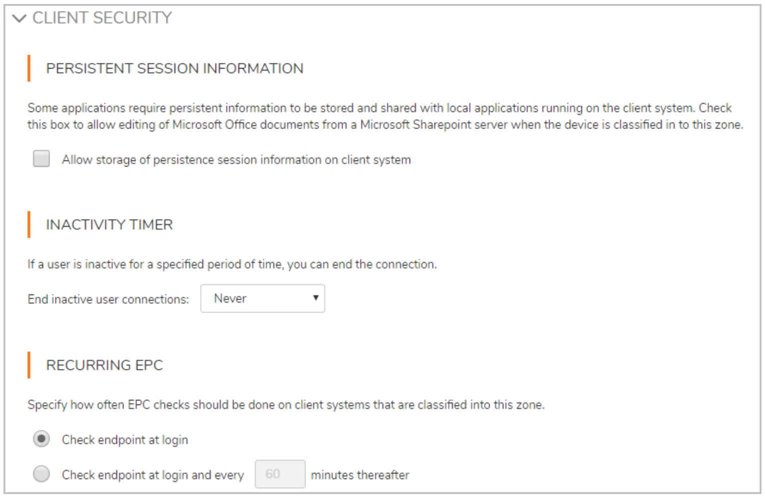
1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.
3. Click the **+** (New) icon and select **Device zone** from the drop-down list.

The **Add Device Zone** page displays.

4. In the **Name** field, type a meaningful name for the zone (for example, *Windows firewall required*). If a zone will be referenced by mobile device users, keep the name short so that all of it is visible on the mobile device.
5. (Optional) In the **Description** field, type a descriptive comment about the zone.
6. In the **All Device Zone Profiles** list, select the check box for any device profiles that you want to require in the zone, and then click the check mark icon. Only one of the profiles in the **In Use** list needs to match for the device to be placed in the zone you are creating.
7. If there are no device profiles previously configured, click **+** (New) icon to add one. See Defining Device Profiles for a Zone for more information on creating profiles.
8. In the **Access method restrictions** area, select which access methods, if any, will not be allowed for clients that are classified into this zone.
9. Specify whether a **Data protection** agent is required.
10. Check the top check box in the **Device Authorization** area to require users to authorize their personal device before a VPN connection is established. By default, this check box is always unchecked (disabled).
11. To change the authorization terms that users must agree to, type the desired authorization terms in the **Terms** section of the **Device Authorization** area.

    The **Device Authorization** check box must be checked to edit the terms.
12. By default, a user authorization expires 180 days after the device was last used. When device authorization is enabled, you can disable zone authorization expiration by unchecking the expiration check box or change the number of days before expiration by typing the desired number of days.



CLIENT SECURITY

PERSISTENT SESSION INFORMATION

Some applications require persistent information to be stored and shared with local applications running on the client system. Check this box to allow editing of Microsoft Office documents from a Microsoft Sharepoint server when the device is classified in to this zone.

□ Allow storage of persistence session information on client system

INACTIVITY TIMER

If a user is inactive for a specified period of time, you can end the connection.

End inactive user connections: Never

RECURRING EPC

Specify how often EPC checks should be done on client systems that are classified into this zone.

● Check endpoint at login

○ Check endpoint at login and every 60 minutes thereafter

13. Expand the **Client security** area.
14. In the **Persistent Session Information** group, enable **Allow storage of persistence session information on client system** if you want persistent information to be stored with local applications running on the client system.

15. By default, user connections to a device zone are not dropped when the connection is inactive. However, a inactivity timer can be set In the **Inactivity timer** area to end the connection after a set period of inactivity. The inactivity timer interval can be set from 1 minute to 24 hours. By default, in a Zone Inactivity timeout is set to Never.

    ⓘ | **NOTE:** In earlier releases, the Inactivity Timer was part of Community attributes.

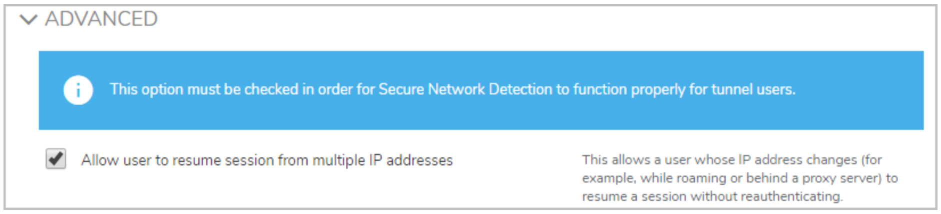
16. In the **Recurring EPC** area, you can select how often EPC checks are done:

    - **Check endpoint at login** (default) – only once (at login)
    - **Check endpoint at login and then every <*n*> minutes for the duration of the session**

    See Performing Recurring EPC Checks: Example for a description of a scenario where the appliance repeatedly checks for the presence of a USB device: when the check fails, the session ends. By default, the end point is checked at login.

17. The connection between devices and the appliance can handle interruptions—such as suspending a session and later resuming it, or temporarily losing connectivity—without requiring that users reauthenticate, as long as the device is using the same IPv4 or IPv6 IP address.

    To allow users to resume sessions from a different IP address—for example, when roaming from one IP subnet to another by plugging into another part of your network—select the **Allow user to resume session from multiple IP addresses** check box in the **Advanced** area.



ADVANCED

This option must be checked in order for Secure Network Detection to function properly for tunnel users.

☑ Allow user to resume session from multiple IP addresses

This allows a user whose IP address changes (for example, while roaming or behind a proxy server) to resume a session without reauthenticating.

18. Click **Save**.

ⓘ | **NOTE:** For information on how to copy or delete an EPC zone, see Adding, Editing, Copying, and Deleting Objects in AMC.

Creating a Deny Zone

Deny zones are evaluated first. If there is a device profile match (for example, if a certain file or registry key is found on the device), the user is denied access and logged out.

To define a Deny zone:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

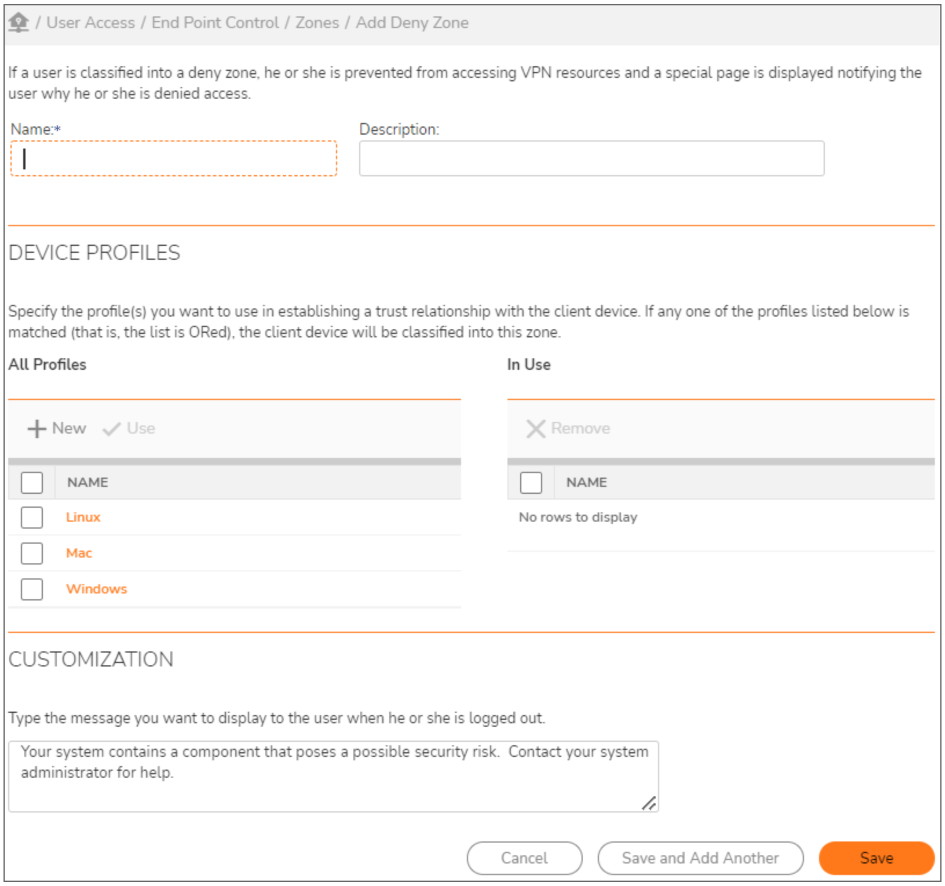
2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.

   The **Zones and Profiles** page displays.

3. Click the **+** (New) icon.

4. Select **Deny zone** from the dropd-own list.

   The **Add Deny Zone** page displays.



If a user is classified into a deny zone, he or she is prevented from accessing VPN resources and a special page is displayed notifying the user why he or she is denied access.

Name:*

Description:

DEVICE PROFILES

Specify the profile(s) you want to use in establishing a trust relationship with the client device. If any one of the profiles listed below is matched (that is, the list is ORed), the client device will be classified into this zone.

All Profiles

□	NAME
□	Linux
□	Mac
□	Windows

In Use

□	NAME
	No rows to display

CUSTOMIZATION

Type the message you want to display to the user when he or she is logged out.

Your system contains a component that poses a possible security risk. Contact your system administrator for help.

5. In the **Name** field, type a meaningful name for the zone (for example, *Google Desktop present*).
6. (Optional) In the **Description** field, type a descriptive comment about the zone.
7. In the **All Profiles** list, select the check box for any device profiles that you want to require in the zone, and then click the checkmark icon. (Only one of the profiles in the **In Use** list needs to match in order for the device to be placed in the Deny zone you are creating.)

   For example, the device profile definition might require that the application `GoogleDesktop.exe` be running. If `GoogleDesktop.exe` is found on the device, the device is a match for the **Deny** zone you named *Google Desktop present*, and the user is denied access and logged off.
8. If there are no device profiles previously configured, click **+** (New) icon to add one. See Defining Device Profiles for a Zone for more information on creating profiles.
9. At the **Customization** section at the bottom of the **Zone Definition** page, you can customize the message that denied users see when they are logged out (for example, `Your system is running Google Desktop, which poses a security risk`).
10. Click **Save**.

For information on how to copy or delete an EPC zone, see Adding, Editing, Copying, and Deleting Objects in AMC.

Creating a Quarantine Zone

For devices that cannot be classified—that is, they do not match any of the **Deny** or **Device** zone profiles—you can create a **Quarantine** zone. You can offer a user whose device is classified into this zone Web links and an explanation, for example, of how to bring his or her device into compliance with your security policies, or how to configure a system for EPC interrogation.

ⓘ **NOTE:** Only one **Quarantine** zone per community can be defined (you can create multiple **Deny** and **Standard** zones).

When you configure a community, you choose the fallback zone for devices that cannot be classified: they can either be placed in the **Default** zone or a **Quarantine** zone. For more information, see Using End Point Control Restrictions in a Community

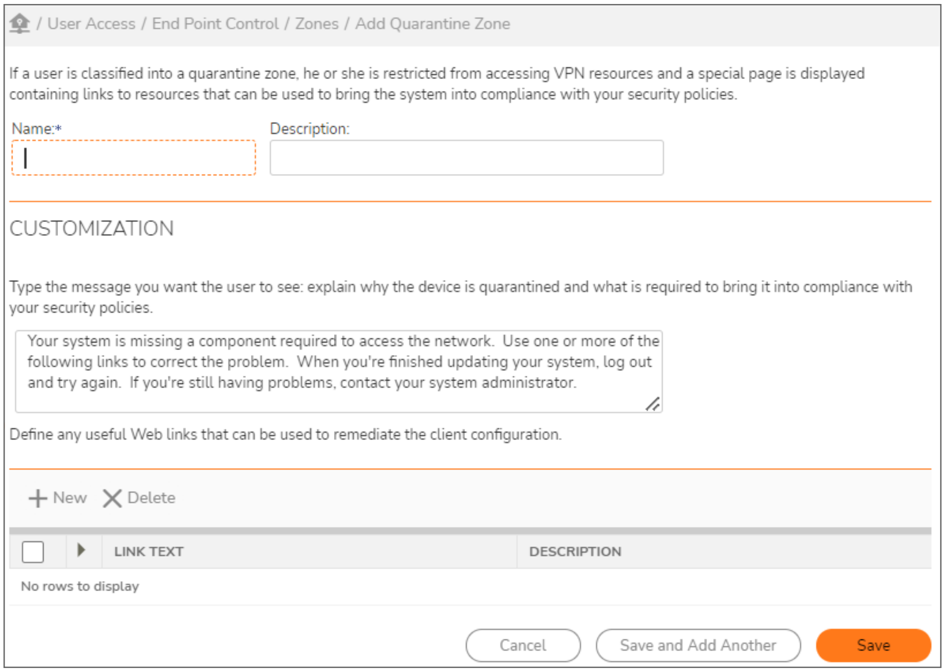
To define a Quarantine zone:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.

   The **Zones and Profiles** page displays.
3. Click the **+** (New) icon.
4. Select **Quarantine zone** from the drop-down list.

   The **Add Quarantine Zone** page displays.



/ User Access / End Point Control / Zones / Add Quarantine Zone

If a user is classified into a quarantine zone, he or she is restricted from accessing VPN resources and a special page is displayed containing links to resources that can be used to bring the system into compliance with your security policies.

Name:*

Description:

CUSTOMIZATION

Type the message you want the user to see: explain why the device is quarantined and what is required to bring it into compliance with your security policies.

Your system is missing a component required to access the network. Use one or more of the following links to correct the problem. When you're finished updating your system, log out and try again. If you're still having problems, contact your system administrator.

Define any useful Web links that can be used to remediate the client configuration.

□	LINK TEXT	DESCRIPTION

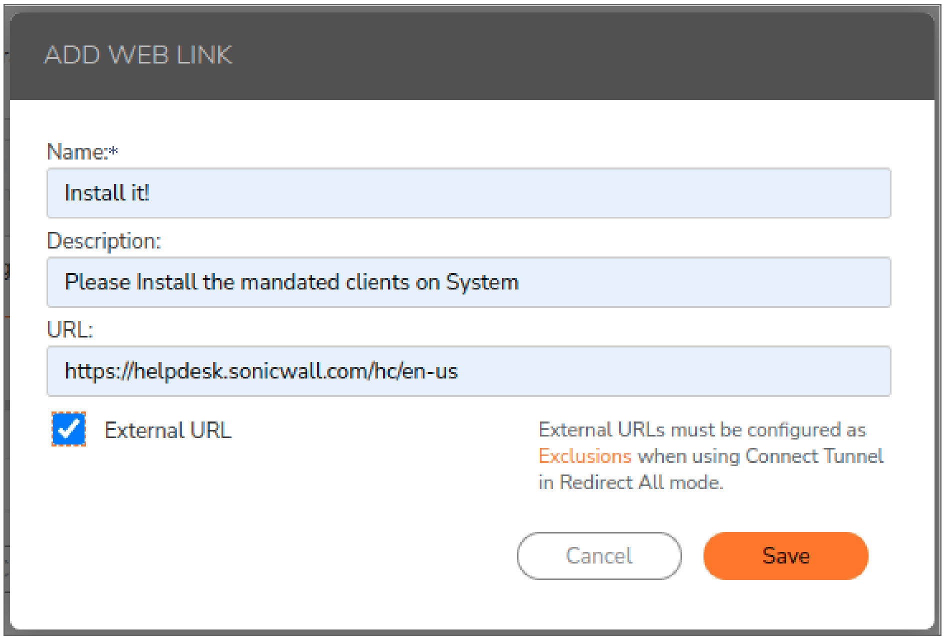
No rows to display

5. In the **Name** field, type a meaningful name for the zone.

6. (Optional) In the **Description** field, type a descriptive comment about the zone.
7. In the **Customization** area, type the message you want quarantined users to see. You might offer an explanation for why a device was placed in quarantine and what is required to make it comply with your security policies.

   Remediation steps for devices that are placed in a **Quarantine** zone should probably include information on how to configure a system for EPC interrogation.
8. Add any Web links that can help users bring their devices into compliance. This can be a mixture of public and private URLs:
   - A public address might reference an Internet URL from which the user can download a software component, such as a Java Virtual Machine. Public resources are normally redirected through the appliance; prevent this redirection by adding the resource in the exclusion list. See Using the Exclusions for instructions.
   - A private address might reference an intranet URL containing the latest virus definitions. In this case, rules are automatically created to give users access to the URL you specify and to prevent them from accessing any other resources.
9. Enable the **External URL** check box.

   ⓘ | **NOTE:** Enable the **External URL** check box only if the URL is in public network.



ADD WEB LINK

Name:* Install it!

Description: Please Install the mandated clients on System

URL: https://helpdesk.sonicwall.com/hc/en-us

☑ External URL

External URLs must be configured as Exclusions when using Connect Tunnel in Redirect All mode.

ⓘ | **NOTE:**

- When the **External URL** check box is enabled:
  - The automatic URL resource is considered as external and webURL config element attribute is set to true.
  - The URL is displayed as-is without any translation, client reaches the URL directly.
- When the **External URL** check box is disabled:

- The webURL config element attribute is set to falce.
- The translated URL is displayed and the client reaches the URL through appliance.

10. Click **Save** or **Save and Add Another**.
11. Create an EPC Standard zone that requires the device profile from the preceding step.
12. Add the configured Standard Zone to a Community and make Quarantine Zone as Zone Fallback options for the same Community. See Using End Point Control Restrictions in a Community section in admin guide.
13. Apply Pending Changes.

Verifying the URLs

To verify the URLs:

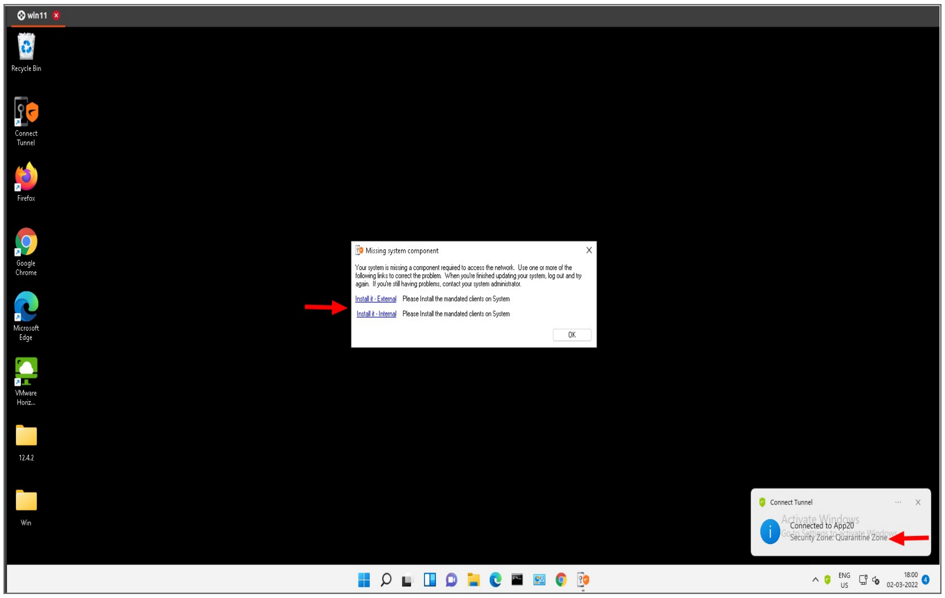
1. Login to Workplace or connect tunnel through the realm associated with the configured community.
2. Ensure to check that the EPC Zone classification fails and Zone falls back to Quarantine Zone.

   ⓘ | **NOTE:**

   - Configure external URLs as Resource Exclusions for CT sessions in Redirect All Tunnel Mode. If not, irrespective of being configured as “External URL”, the links will still be redirected to SMA in Redirect All Tunnel Mode.

   The URLs are displayed without translation.

   Connect Tunnel



Missing system component

Your system is missing a component required to access the network. Use one or more of the following links to correct the problem. When you're finished updating your system, log out and try again. If you're still having problems, contact your system administrator.

Install it - External Please Install the mandated clients on System

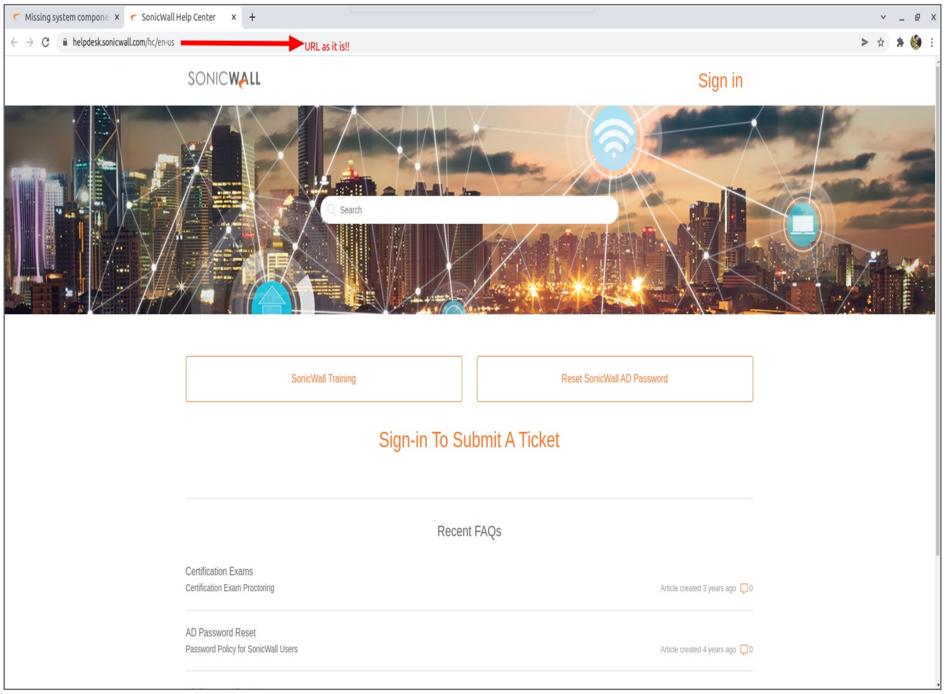
Install it - Internal Please Install the mandated clients on System

Connect Tunnel

Connected to App20

Security Zone: Quarantine Zone

WorkPlace:


Missing system compone
SonicWall Help Center
helpdesk.sonicwall.com/hc/en-us
SONICWALL
Sign in
Search
SonicWall Training
Reset SonicWall AD Password
Sign-in To Submit A Ticket
Recent FAQs
Certification Exams
Certification Exam Proctoring
Article created 3 years ago 0
AD Password Reset
Password Policy for SonicWall Users
Article created 4 years ago 0

URL as it is!!

Configuring the Default Zone

AMC provides a global **Default** zone that serves as a fail-safe to either allow or block VPN access for any connection requests that don't match the other zones you set up. When the appliance receives a connection request that it can't classify into a zone—meaning it can't identify the client device's operating system, browser, or other attributes—that device is automatically placed in the **Default** zone. You can choose whether to grant or deny VPN access to users whose devices are assigned to the **Default** zone.

Unlike other zones, the **Default** zone does not include device profiles, but it can be configured to require the presence of a data protection agent. The **Default** zone is implicitly present in every community configured in AMC.

To provide a limited degree of access to users whose connection requests don't meet your criteria for a trusted relationship, you can include the **Default** zone in a restrictive access control rule. For example, you could let users access their email by including the **Default** zone in a "permit" access control rule limited to Web browsers connecting to Outlook Web Access.

If a restrictive access policy that requires a high degree of trustworthiness and does not allow connection requests unless they are explicitly defined, setting the **Default** zone to **Block VPN access** is the best strategy. Keep in mind that if your other zones and access control rules inadvertently omit legitimate users, the **Default** zone will block them without exception.

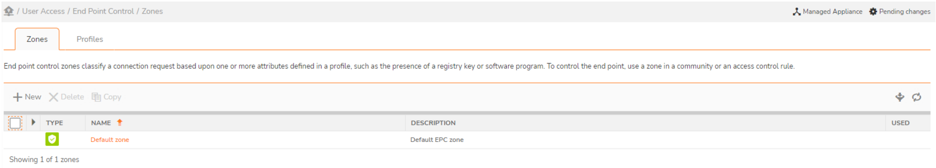
To configure the Default zone:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.

   The **Zones and Profiles** page displays.



/ User Access / End Point Control / Zones

Managed Appliance · Pending changes

Zones · Profiles

End point control zones classify a connection request based upon one or more attributes defined in a profile, such as the presence of a registry key or software program. To control the end point, use a zone in a community or an access control rule.

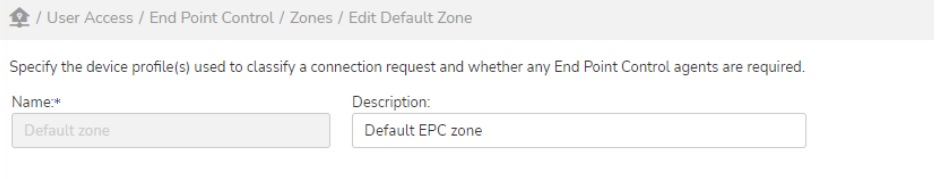
+ New · Delete · Copy

□	TYPE	NAME	DESCRIPTION	USED
	✓	Default zone	Default EPC zone	

Showing 1 of 1 zones

3. Click **Default zone** in the table.

   The **Edit Default Zone** page displays.



/ User Access / End Point Control / Zones / Edit Default Zone

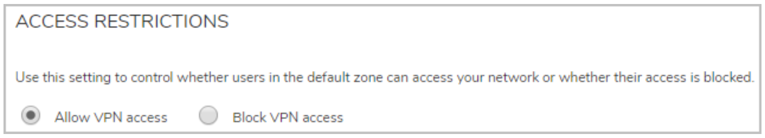
Specify the device profile(s) used to classify a connection request and whether any End Point Control agents are required.

Name:* Default zone

Description: Default EPC zone

The **Name** field is dimmed as the name for this zone cannot be changed.

4. In the **Access restrictions** section, select whether the appliance will **Allow VPN access** or **Block VPN access** for devices that are placed in the **Default** zone. If you select **Block VPN access**, users who are assigned to the **Default** zone are logged off of the appliance.

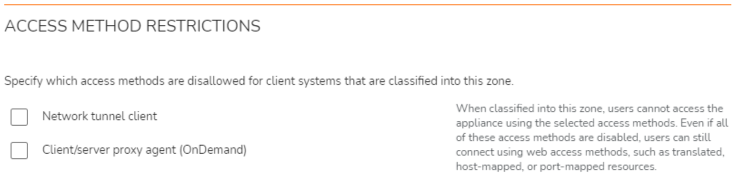


ACCESS RESTRICTIONS

Use this setting to control whether users in the default zone can access your network or whether their access is blocked.

● Allow VPN access ○ Block VPN access

5. In the **Access method restrictions** section, specify which access methods, if any, will not be allowed for clients that are classified into this zone.



ACCESS METHOD RESTRICTIONS

Specify which access methods are disallowed for client systems that are classified into this zone.

□ Network tunnel client

□ Client/server proxy agent (OnDemand)

When classified into this zone, users cannot access the appliance using the selected access methods. Even if all of these access methods are disabled, users can still connect using web access methods, such as translated, host-mapped, or port-mapped resources.

6. Expand the **Client security** section.

7. In the **Persistent Session Information** group, enable **Allow storage of persistence session information on client system** if you want persistent information to be stored with local applications running on the client system.

8. By default, user connections to a device zone are not dropped when the connection is inactive. However, a inactivity timer can be set In the **Inactivity timer** area to end the connection after a set period of

inactivity. The inactivity timer interval can be set from 1 minute to 24 hours. By default, in a Zone Inactivity timeout is set to Never.

ⓘ | **NOTE:** In earlier releases, the Inactivity Timer was part of Community attributes.

9. In the **Recurring EPC** section, you can specify how often EPC checks are done. Select:
    - **Check endpoint at login** to perform an EPC check only once (at login)
    - **Check endpoint at login and every** <*n*> **minutes thereafter** at login and then every <*n*> minutes for the duration of the session.
10. Expand the **Advanced** section.
11. The connection between devices and the appliance can handle interruptions—such as suspending a session and later resuming it, or temporarily losing connectivity—without requiring that users reauthenticate, as long as the device is using the same IPv4 or IPv6 IP address.

    To allow users to resume sessions from a different IP address—for example, when roaming from one IP subnet to another by plugging into another part of your network—select the **Allow user to resume session from multiple IP addresses** check box in the **Advanced** area.

    ⓘ | **NOTE:** For Secure Network Detection to work, this check box must be checked to allow users to resume sessions from multiple IP addresses.
12. Click **Save**.

Defining Device Profiles for a Zone

A device profile establishes a trust relationship with a client device by looking for one or more attributes, such as an antimalware program, application, or Windows registry entry. Device profiles can be referenced by one or more zones.

A device profile can be defined to detect only one attribute on a client computer, or it can require multiple attributes. When a device profile references multiple attributes, each of those attributes must be present on a client computer for there to be a match.

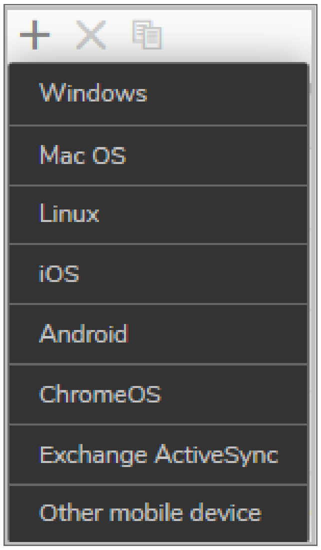
ⓘ | **NOTE:** For information on how to copy or delete a device profile, see Adding, Editing, Copying, and Deleting Objects in AMC.

To define a device profile for a zone:

1. In the AMC, navigate to **User Access > End Point Control**.

    The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.

    The **Zones and Profiles** page displays.
3. Click the **+** (New) icon.



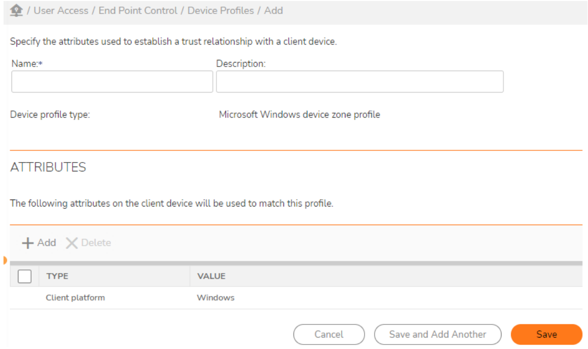
4. Select one of the SMA EPC-supported device profiles:
   - Windows
   - Mac OS
   - Linux
   - iOS
   - Android
   - ChromeOS
   - Exchange ActiveSync
   - Other mobile device

     ⓘ **NOTE:** You can also match a policy as a Platform in an Access Control Rule, which does not require End Point Control.

   The **Add Device Profile page** displays. The available options will depend on the device profile you selected.

   - Device Profile Definition for Microsoft Windows
   - Device Profile Definition for ChromeOS

Device Profile Definition For Microsoft Windows



/ User Access / End Point Control / Device Profiles / Add

Specify the attributes used to establish a trust relationship with a client device.

Name:*

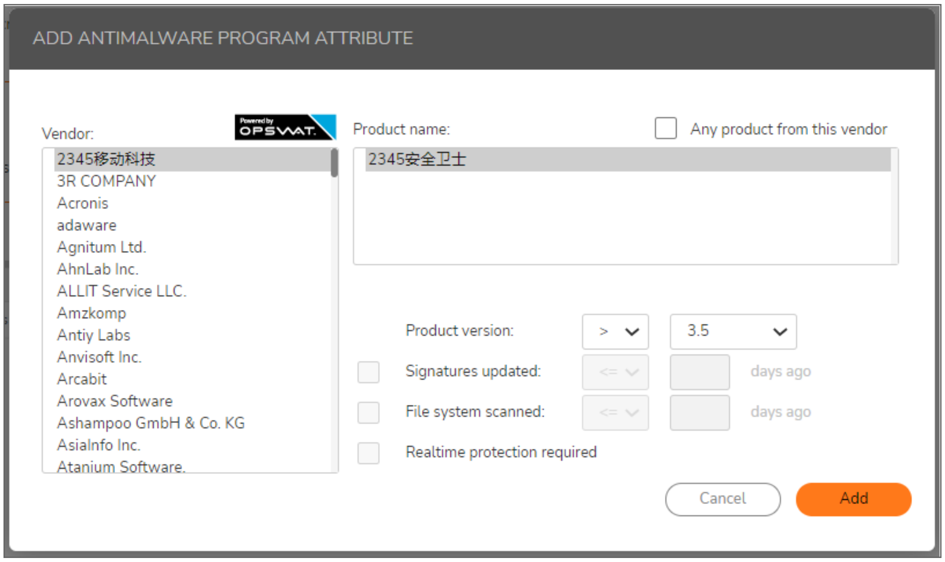
Description:

Device profile type: Microsoft Windows device zone profile

ATTRIBUTES

The following attributes on the client device will be used to match this profile.

TYPE	VALUE
Client platform	Windows



ADD ANTIMALWARE PROGRAM ATTRIBUTE

Vendor:

- 2345移动科技
- 3R COMPANY
- Acronis
- adaware
- Agnitum Ltd.
- AhnLab Inc.
- ALLIT Service LLC.
- Amzkomp
- Antiy Labs
- Anvisoft Inc.
- Arcabit
- Arovax Software
- Ashampoo GmbH & Co. KG
- Asialnfo Inc.
- Atanium Software.

Product name: □ Any product from this vendor

2345安全卫士

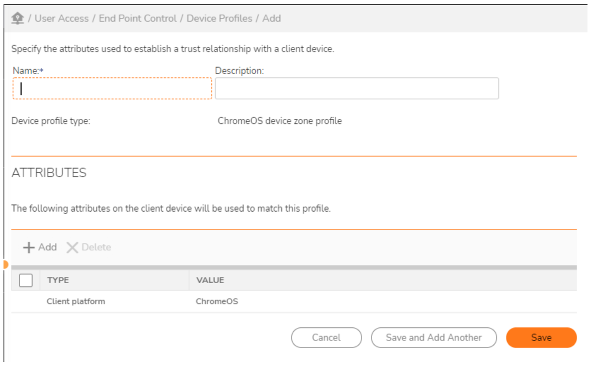
Product version: > 3.5

□ Signatures updated: <= days ago

□ File system scanned: <= days ago

□ Realtime protection required

Device Profile Definition For ChromeOS



/ User Access / End Point Control / Device Profiles / Add

Specify the attributes used to establish a trust relationship with a client device.

Name:*

Description:

Device profile type: ChromeOS device zone profile

ATTRIBUTES

The following attributes on the client device will be used to match this profile.

TYPE	VALUE
Client platform	ChromeOS

5. In the **Name** field, enter a name for the device profile.
6. (Optional) In the **Description** field, enter a descriptive comment about the device profile.
7. From the **Value** section, select the attributes that you want for the device profile.

8. After selecting each attribute, click **Add**.

   The attribute is added to the **Current attributes** list at the bottom of the page.

   - The available attributes depend on the device profile you selected; Antimalware program and Personal Firewall Program is available only for users who are licensed with the Advanced EPC feature.
   - Where multiple entries are allowed for an attribute, note whether a device profile must match *all* (**and**) or match *any* (**or**) items on the device.

   Detailed descriptions of the attributes and the platforms on which they are available are inDevice Profile Attributes.

9. Click **Save**.

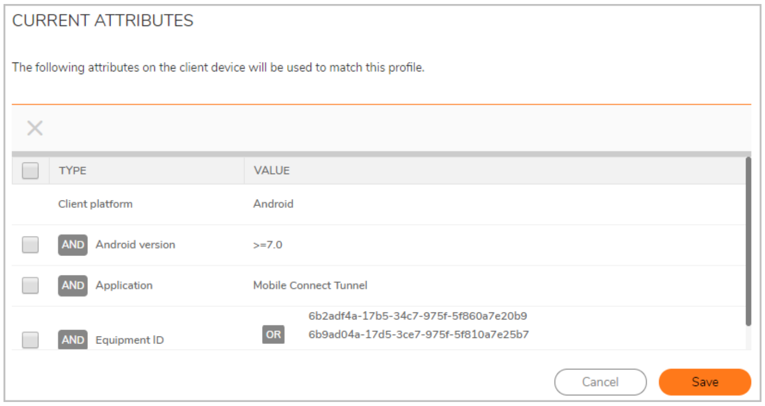
Device Profile Attributes

A device profile can have several attributes: the platforms on which it can be used and whether multiple attributes of the same type (where allowed) are ORed or ANDed:

- Device Profile Attributes: ChomeOS version
- Device Profile Attributes: Android/Windows/ Mac/ Linux/ ChromeOS application
- Device Profile Attributes: Android version
- Device Profile Attributes: Antimalware program (Advanced EPC only)
- Device Profile Attributes: client certificate
- Device Profile Attributes: directory name
- Device Profile Attributes: iOS version
- Device Profile Attributes: macOS version
- Device Profile Attributes: Personal firewall program (Advanced EPC only)
- Device Profile Attributes: Windows domain
- Device Profile Attributes: Windows registry entry
- Device Profile Attributes: Equipment ID
- Device Profile Attributes: file name
- Device Profile Attributes: Microsoft Intune
- Device Profile Attributes: Linux Kernel version

There are a few things to note about these attributes:

- The attributes from which you can choose differ depending on the platform you selected for your device profile.
- Users who have Advanced EPC can pick from a wide range of security programs.
- Where multiple entries are allowed for an attribute, a device profile must either match *all* (**and**) or *any* (**or**) items on the device.

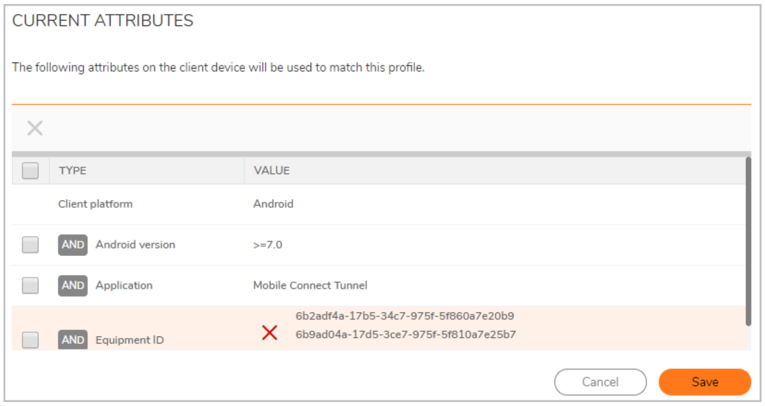


CURRENT ATTRIBUTES

The following attributes on the client device will be used to match this profile.

□	TYPE	VALUE
	Client platform	Android
□	AND Android version	>=7.0
□	AND Application	Mobile Connect Tunnel
□	AND Equipment ID	OR 6b2adf4a-17b5-34c7-975f-5f860a7e20b9 6b9ad04a-17d5-3ce7-975f-5f810a7e25b7

- To delete an item in the list, select the check box in the left column and click **Delete**. To delete a single (**or**) item, move your pointer to the left of the item you want to delete and click the red **X** icon that appears.



CURRENT ATTRIBUTES

The following attributes on the client device will be used to match this profile.

□	TYPE	VALUE
	Client platform	Android
□	AND Android version	>=7.0
□	AND Application	Mobile Connect Tunnel
□	AND Equipment ID	✕ 6b2adf4a-17b5-34c7-975f-5f860a7e20b9 6b9ad04a-17d5-3ce7-975f-5f810a7e25b7

Device Profile Attributes: ChomeOS Version

ChromeOS version	Platform	Match
Type the major and minor versions, and the build number for the operating system. The comparison **Operator** applies to all three values. To specify all versions, enter “greater than or equal to” (**>=**) as the **Operator**, and then type the major version number in the **Major** field and the minor version number in the **Minor** field. You can also specify the **Build** and the **Patch** numbers. For more information, see Using Comparison Operators with Device Profile Attributes.	ChromeOS	AND (Match all)

Device Profile Attributes: Android/Windows/ Mac/ Linux/ ChromeOS Application

Android/ Windows/ Mac/ Linux/ ChromeOS Application	Platform	Match
Type the application name with extensions that EPC should check for in this profile.	Android Windows Mac Linux ChromeOS	AND (Match all)

Device Profile Attributes: Android Version

Android version	Platform	Match
Type the major and minor versions, and the build number for the operating system. The comparison **Operator** applies to all three values. To specify all versions, enter “greater than or equal to” (**>=**) as the **Operator**, and then type the major version number in the **Major** field and the minor version number in the **Minor** field. For more information, see Using Comparison Operators with Device Profile Attributes.	Android	AND (Match all)

Device Profile Attributes: Antimalware Program (Advanced EPC Only)

Antimalware program	Platform	Match
(This attribute is available only if you have Advanced EPC). Select the antimalware programs that EPC should check for in this profile. See Advanced EPC: Extended Lists of Security Programs for more information. If you don’t have Advanced EPC, or if you don’t see the security programs that your users require, you can still specify programs by adding them to a device profile using another attribute, such as *Application* or *Windows registry entry*. Few Antimalware Program that is used are: McAfee, Sophos, Bitdefender, ESET	Windows macOS Linux	OR (Match any)

Device Profile Attributes: Client Certificate

Client certificate	Platform	Match
Select a Certificate Authority from the drop-down menu in the **CA certificate** area. (See Importing CA Certificates if the CA you want to use is not listed). A client device will match this profile as long as the appliance is configured with the root certificate for the CA that issued the client certificate to your users. Select the certificate store(s) you want searched: • **System store only** specifies that only the system store (*HKLM\SOFTWARE\Microsoft\SystemCertificates*) is searched • **System store and user store** specifies that the system store is searched first, followed by the user store (*HKCU\Software\Microsoft\SystemCertificates*) ⓘ | **NOTE:** • A device profile can contain only one client certificate attribute. • The system store cannot be searched unless the user has administration privileges on the client device. • Enable the option “Trust” to trust Intermediate CAs without verifying the entire chain.	Windows macOS Apple iOS Android Linux Chrome OS	OR (Match any)

Device Profile Attributes: Directory Name

Directory name	Platform	Match
Type the name of a directory that must be present on the hard disk of the device. Directory names are not case-sensitive. ⓘ **NOTE:** When creating a device profile for jailbroken iOS devices, be sure to configure a denied EPC zone for the profile and bind this zone to at least one community. ⓘ **NOTE:** The directory must be accessible to the user logging in. If the directory is not accessible to the user, the End Point Control evaluation will fail.	Windows macOS Linux Apple iOS Android Chrome OS	AND (Match all)

Device Profile Attributes: Equipment ID

Equipment ID	Platform	Match
Type the identifier for the device or use variables to define the identifier based on user attributes. You can choose to allow access to users who do not have any registered devices on the external AD/LDAP server. Typically this would be done to allow a user access until their device identifier can be registered. Whether or not you choose to allow access, all requests for access that come from unregistered devices will be logged in the Unregistered Device Log.	Windows macOS Linux Apple iOS Android Chrome OS	AND (Match all)

Device Profile Attributes: File Name

File name	Platform	Match

Type the name of a file (including its extension and full path) that must be present on the hard disk of the device. File names are not case-sensitive. You can use environment variables (such as `%windir%` or `%userprofile%`), or wildcard characters (`*` and `?`). You can optionally specify a **File size** or the date and time (GMT) the file was **Last modified**. Both of these options use a comparison **Operator**; for more information and examples, see Using Comparison Operators with Device Profile Attributes. The file's modification date and time can be specified as an **Absolute** or **Relative value**. The device profile can be configured to **validate file integrity** using an MD5 or SHA-1 hash (valid on all platforms), or use a Windows catalog file to validate Windows system files. Device profiles that check for the name of the file(s) used by jailbroken or rooted devices include: • For jailbroken Apple iOS devices, the file name is `cydia`. • For rooted Android devices, the file names are `/system/bin/su` and `/system/xbin/su`. ⓘ **NOTE:** If creating a device profile for jailbroken iOS devices or rooted Android devices, be sure to configure a denied EPC zone for each profile and bind each of these zones to at least one community. ⓘ **NOTE:** The files and directories must be accessible to the user logging in. If the file is not accessible to the user, the End Point Control evaluation will fail.	Windows macOS Linux Apple iOS Android Chrome OS	AND (Match all)

Device Profile Attributes: IOS Version

iOS version	Platform	Match
Type the major and minor versions, and the build number for the operating system. For example, enter **Major** 5, **Minor** 0, and **Build** 9A405 for the iOS 5.0.1 build 9A405 version. The comparison **Operator** applies to all three values. To specify all versions of 5.0, for example, enter "greater than or equal to" (**>=**) as the **Operator**, and then type `5`in the **Major** and `0` in the **Minor** fields. For more information, see Using Comparison Operators with Device Profile Attributes.	Apple iOS	AND (Match all)

Device Profile Attributes: MacOS Version

macOS version	Platform	Match

Type the major and minor versions, and the build number for the operating system. Examples of versions for macOS are: - v11.X - v10.15 The comparison **Operator** applies to all three values. For example, enter “greater than or equal to” (>=) as the **Operator**, and then type `10` in the **Major** and `5` in the **Minor** fields. For more information, see Using Comparison Operators with Device Profile Attributes.	macOS	AND (Match all)

Device Profile Attributes: Personal Firewall Program (Advanced EPC Only)

Personal firewall program	Platform	Match
(This attribute is available only if you have Advanced EPC). Select the firewall programs that EPC should check for in this profile. See Advanced EPC: Extended Lists of Security Programs for more information. If you don’t have Advanced EPC, or if you don’t see the security programs that your users require, you can still specify programs by adding them to a device profile using another attribute, such as *Application* or *File Name*. Few Antimalware Program that is used are: McAfee, ESET , Intego, Open Door Networks	Windows macOS Linux	OR (Match any)

Device Profile Attributes: Windows Domain

Windows domain	Platform	Match
Type the domain name the computer belongs to in NetBIOS syntax (for example, `mycompany`), without a DNS suffix. Separate multiple entries with a semicolon. The domain can contain wildcard characters (`*` and `?`).	Windows	OR (Match any)

Device Profile Attributes: Windows Registry Entry

Windows registry entry	Platform	Match
Type the **Key name**, and optionally enter a **Value name** and **Data**, and then select a comparison **Operator** for the **Data** field. See Using Comparison Operators with Device Profile Attributes for more information. Wildcards can be used for the value and data, but not for the key. To enter a special character (such as a wildcard or back slash), you must precede it with a back slash.	Windows	AND (Match all)

Device Profile Attributes: Windows Version

Windows version	Platform	Match

Type the major version, minor version, build, and revision number for the operating system. Example major/minor versions, build number, revision number for Windows 10 are: • Windows 10: 10/0/17134/523 The comparison **Operator** applies to all three values. For more information, seeUsing Comparison Operators with Device Profile Attributes.	Windows	AND (Match all)

Device Profile Attributes: Microsoft Intune

Windows version	Platform	Match
Configure the following options: AAD registered, Compliant, Last Sync, Device Owner, and Encrypted. **NOTE:** By default, this attribute is disabled. To enable, in AMC navigate to **User Access > End Point Control > Mobile Device Management Profiles** and configure Microsoft Intune settings.	Windows	AND (Match all)

Device Profile Attributes: Linux Kernel Version

Linux version	Platform	Match
Type the major version, minor version, and build for the operating system. Example major/minor versions, and build number. • Linux: 5.8.66 The comparison **Operator** applies to all three values. For more information, seeUsing Comparison Operators with Device Profile Attributes.	Linux	AND (Match all)

Advanced EPC: Extended Lists of Security Programs

Advanced EPC is an optional component—licensed separately—that provides an extended and detailed list of security programs. You can configure EPC device profiles to check for personal firewall and antimalware programs on clients running the following platforms:

- Microsoft Windows
- macOS
- Linux.

Advanced EPC includes a built-in list of device profiles you can use as it is or modify; see Advanced EPC: Using Preconfigured Device Profiles for more information.

NOTE: The version of OESIS libraries on the client will always be the same as that of OESIS libraries configured on the connecting appliance. If there is any version mismatch, the client installs the OESIS libraries from the appliance.

To add attributes using Advanced EPC:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.

   The **Zones and Profiles** page displays.
3. In the **Device Profiles** section, click the **+** (New) icon.
4. Select an operating system from the drop down list.
5. After giving the profile a **Name** (a **Description** is optional), select the **Type** of program for which EPC should check (for example, *Antimalware program*).
6. Select a **Vendor and Product name**. .
7. Specify an absolute or relative **Product version**.

   Some products are known by several different names. For example, Kaspersky Lab offers a core product named *Kaspersky Anti-Virus* that is also known as *Kaspersky Anti-Virus 2018* and *Kaspersky Anti-Virus 2019*. (When you select a product name that has an asterisk, you'll see a footnote indicating its "core" product name.) Using the name indicated in the footnote is recommended so that you don't have to update your device profile every time a core product is marketed under a new name.
8. There are optional parameters you can use to more narrowly define the security program settings that the device profile requires (not all parameters are available for each program choice—any that are not available are dimmed):

   - **Signatures updated**: Defines how recently the list of antimalware signatures was updated on the client device.
   - **File system scanned**: Defines how recently the client device's disk was scanned using this antimalware program.
   - **Realtime protection required**: If the device profile requires that realtime scanning for viruses and spyware is enabled, select this check box.
9. Click the **Add** button to add an entry to the list at the bottom of the page. When you add additional programs (for example, if you want the device profile to check for any of several programs), the device profile must match *all* (**and**) or *any* (**or**) items on the device. Additional antimalware programs are grouped together, but the device profile requires just one of the programs for a match.
10. Click **Save**.

Advanced EPC: Using Fallback Detection

Fallback detection uses advanced EPC to detect newer vendor software versions than are recognized by OESIS, which allows zone classification to succeed. Fallback detection supplements your fully trusted profiles with EPC definitions for the versions you want to determine fully (for example, Microsoft Security Essentials version 4.x or higher).Fallback detection, which uses the Windows Security Center (WSC), can be configured for Windows-based Antimalware and Personal Firewall products.

For example, users are put in the Trusted zone when they log in with Kaspersky Antivirus. When they update to a newer version of Kaspersky and log in, the WSC fallback will match for the Trusted Fallback zone, and they will be allowed access.

When Secure Mobile Access supports the new Kaspersky version, you can simply update the policy for the Trusted zone to include the new version. This allows the admin to easily distinguish between devices that match a specific antimalware version and those that do not, but do match the Fallback logic.

ⓘ **NOTE:** To use Fall back Detection, device profiles for the Primary EPC zone must be configured with specific versions of antimalware and firewall products and NOT with the **Any product from this vendor** option.

To configure Fallback Detection:

1. Create a new device profile for trusted fallbacks with these value:
   a. In the AMC, navigate to **User Access > End Point Control**.
      The **End Point Control** page displays.
   b. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.
      The **Zones and Profiles** page displays.
   c. In the **Device Profiles** section, click the **+** (New) icon.
   d. Select **Windows** from the drop-down list.
   e. Type the **Name** of the new device profile.
   f. From the **Type** drop-down menu, select **Antimalware program** or **Personal firewall program**.
   g. From the **Vendor** drop-down menu, select the vendor that provides the product.
   h. From the **Product** drop-down menu, select **Other** <***vendor***> <***type***> (for example, **Other Aliant Firewall**).
      Do **NOT** use the **Any product from this vendor** check box.
   i. Set the **Product version** to >= x.
   j. If applicable, enable **Signatures updated** and **Realtime protection required**.
   k. Click **Save**.
2. Create a new Trusted Fallback zone and add the Trusted Fallback profile to this zone.

   Optionally, Trusted and Trusted Fallback profiles can be combined into one zone, depending on your security requirements. However, using a separate Trusted Fallback zone allows you to easily determine when users update software that is not matched by the Trusted zone, so you will know when to add new versions to the Trusted zone.
3. In your community, add the Trusted Fallback zone to the Realms list directly below the Trusted zone.

Advanced EPC: Using Preconfigured Device Profiles

To help you get started with End Point Control, there are several preconfigured device profiles, grouped by operating system, that you can use as is or copy and modify to suit your access policy and resource requirements.

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.

   The **Zones and Profiles** page displays.

Preconfigured Device Profiles

Windows	Mac	Linux

You can use these predefined profiles as a starting point for your own:

- Copy one that matches your environment the closest, and then modify it, changing (for example), the acceptable product versions and the requirement for how recently the list of antimalware signatures was updated on the client device.
- To delete an entire row in the list of current attributes, select the check box for that row and click **Delete**.
- To delete an item in an ORed list (like one of the personal firewall products Kaspersky Lab, for example), move your mouse cursor over the "or" and then click the red "X" that appears.

Using Comparison Operators with Device Profile Attributes

Some device profile attributes can be modified using comparison operators shown in the below table, which is useful in situations such as these:

- Keeping a device profile current with software that is automatically updated on client devices—you don't need to manually change the profile each time the software is updated.
- Specifying that a specific file detected on client machines has a timestamp greater than a certain date and time.
- Specifying that the Windows operating system detected on the client device be greater than or equal to a certain version.

Available Comparison Operators

Operator	Description
<	Less than
<=	Less than or equal to
=	Equal to
!=	Not Equal to
>=	Greater than or equal to
>	Greater than

Comparison operators can be used in conjunction with these device profile attributes:

- File date or time stamp for a specific file
- File size for a specific file
- Registry entry (when value data is selected for a registry key)

- Windows version
- Advanced End Point Control

Example

This example show how to find a file on a PC running Microsoft Windows that has recently been updated.

To specify a relative or absolute file date:

1. In the AMC, navigate to **User Access > End Point Control**.
   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.
   The **Zones and Profiles** page displays.
3. In the **Device Profiles** section, click the **+** (New) icon.
4. Select **Windows** from the drop-down list.
5. Type a meaningful name for the device profile in the **Name** field.
6. (Optional) In the **Description** field, type a descriptive comment about the device profile.
7. In the **Add** attribute(s) area, select **File name** in the **Type** list.
8. In the **File name** field, type `weekly_timesheet.xls`. Here are two examples of how to specify a time stamp for the file:
   - To specify that *weekly_timesheet.xls* has been updated within the last five days, select <= in the **Last modified** list, click **Relative**, and then type `5` in the field.
   - To specify that the file was updated after June 1, 2017, select >= in the **Last modified** list, click **Absolute**, and then type `06/01/2017` in the fields.
9. Click **Add to Current Attributes**, and then click **Save**.

Using End Point Control with the Connect Tunnel Client

You can use End Point Control on devices that connect to the appliance using the Connect Tunnel client. As with other access methods, EPC for the Connect Tunnel client supports the use of device profiles and EPC zones.

Performing Recurring EPC Checks: Example

A connection request is classified into an EPC zone based on attributes defined in a device profile. This check is always performed when the user logs in; in addition, you have the option of checking at regular intervals whether a device continues to match the profile for a particular zone.

An example illustrates how this setting might be used. In this scenario the system administrator has given each systems engineer in the organization a USB device that provides access to resources protected by the SMA appliance. This provides two-factor authentication: During a user’s session, the appliance repeatedly checks for the presence of a client certificate associated with a USB device: if the check fails, the session ends. Since an essential part of the user’s authentication (the client certificate) is on the USB device, authentication data does not remain on the system when the systems engineer removes the key.

Here's how it looks from the systems engineer's perspective:

1. Insert your personal USB device into any desktop or laptop device (trusted or untrusted).
2. Enter your PIN number.
3. Log in for access to the VPN and authenticate. The SMA appliance checks for your client certificate when you log in and at regular intervals thereafter (the interval is set by the SMA appliance administrator). When the USB device is removed, the check fails and the connection is ended.

ⓘ **NOTE:** It's important for users to understand that their connectivity depends on the presence of the USB device. For this reason they should also not leave the USB device plugged in and unattended.

Here's an overview of the configuration steps the administrator must take:

1. To establish a trust relationship between the USB device and the appliance, you must reference a root CA certificate in the EPC device profile. If it's not already present, import the certificate to the appliance (click **SSL Settings** in the main navigation menu, and then click **Edit** in the **CA Certificates** area).
2. Using Appliance Management Console, create a device profile for Windows, Mac, or Linux devices to check for the presence of a client certificate on the USB devices you plan to distribute. The certificate must descend from the root certificate from *Step 1*. When creating a device profile for Windows, ensure both system and user certificate stores are searched.
3. Create an EPC Standard zone that requires the device profile from the preceding step.
4. When you are defining the zone, specify in the **Recurring EPC** area at what intervals EPC will check the client systems that are classified into this zone.
5. A device for which there is no profile match—the client certificate does not descend from the root CA certificate identified in the first step, or the USB device has no certificate—will "fall through" to either the **Default** zone or a **Quarantine** zone:
   - To deny access to any connection requests that don't meet your criteria, configure the Default zone to simply deny access. In the **Access restrictions** area on the **Zone Definition** page, select **Block VPN access**.
   - If you prefer, you can create a **Quarantine** zone and customize the message users see; for example, you may want to explain what is required to bring the user's system into compliance with your security policies.

Microsoft Intune

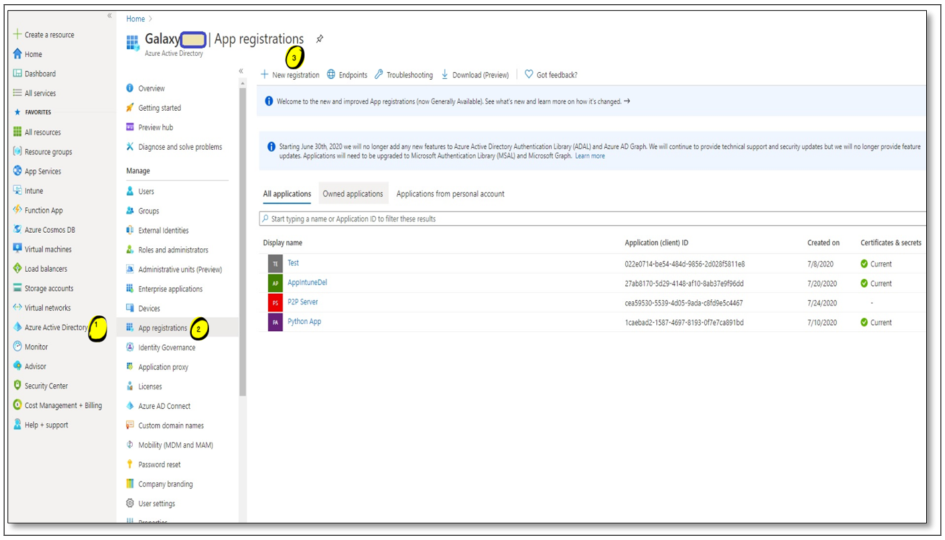
SMA is enhanced to support Microsoft Intune. Microsoft Intune is a Microsoft cloud-based management solution for mobile device and operating system management.From 12.4.2 onwards, the SMA and Microsoft Intune integration is supported for MacOS based managed devices.

For creating MS Intune Windows and Mac profile attributes see Configuring Microsoft Intune in AMC.

Configuring Microsoft Intune

To configure Microsoft Intune:

1. Log in to Azure account as Administrator.
2. Navigate to **Azure Active Directory > App registration > New registration**.

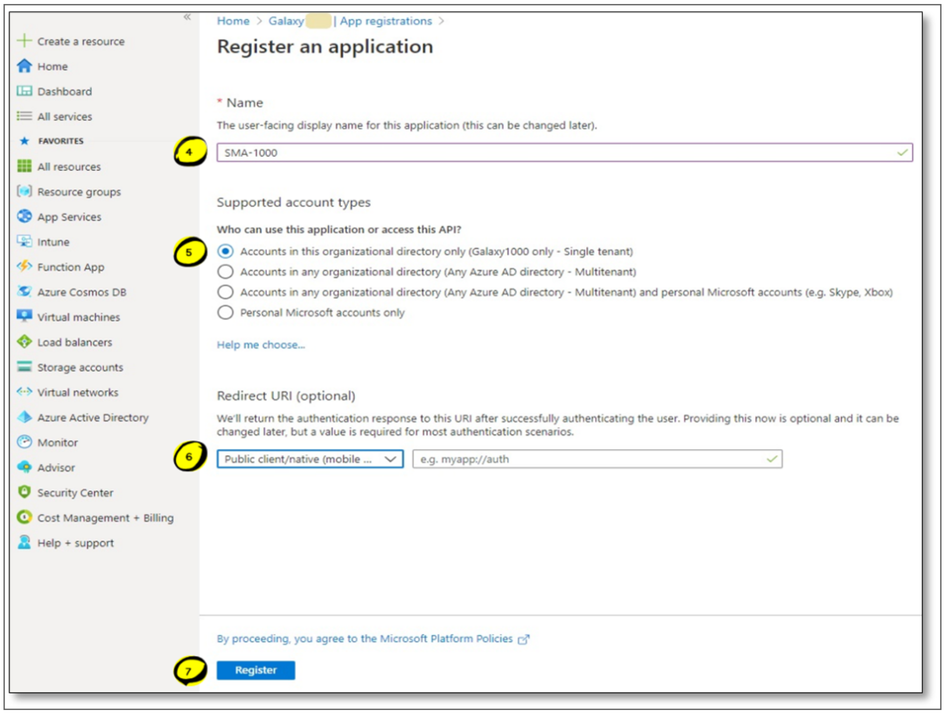


Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Display name	Application (client) ID	Created on	Certificates & secrets
TE Test	022e0714-be54-484d-9856-2d028f5811e8	7/8/2020	✓ Current
AP AppIntuneDel	27ab8170-5d29-4148-af10-8ab37e9f96dd	7/20/2020	✓ Current
PS P2P Server	cea59530-5539-4d05-9ada-c8fd9e5c4467	7/24/2020	-
PA Python App	1caebad2-1587-4697-8193-0f7e7ca891bd	7/10/2020	✓ Current

3. Specify the details as shown in the below image and click **Register**.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

SMA-1000

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Galaxy1000 only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

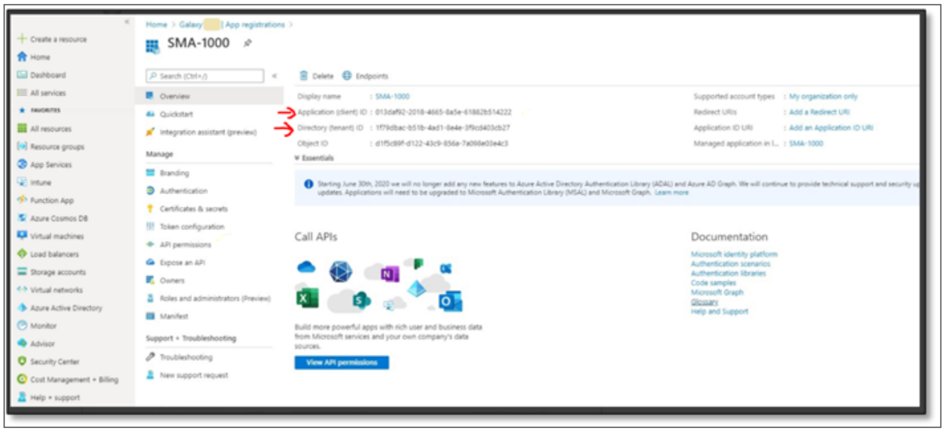
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... e.g. myapp://auth

By proceeding, you agree to the Microsoft Platform Policies

4. After successful registration, **Application**(**Client ID**), **Directory** (**Tenant ID**) will be displayed, note it down for further usage.



Display name : SMA-1000
Application (client) ID : 013daf92-2018-4665-8a5e-61882b514222
Directory (tenant) ID : 1f79dbac-b51b-4ad1-8e4e-3f9cd403cb27
Object ID : d1f5c89f-d122-43c9-856a-7a098e03e4c3

Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : SMA-1000

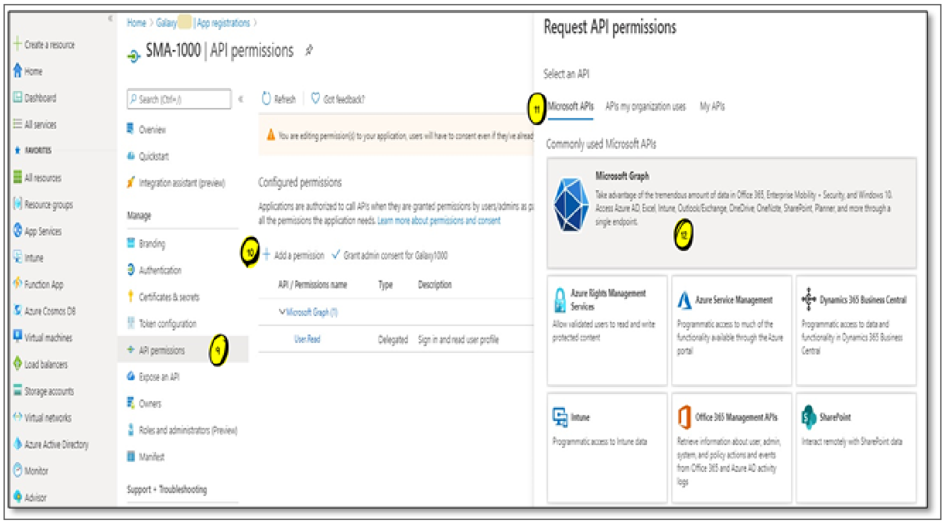
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

5. To set the permissions, select **API permissions** option under registered application and click **+Add a permission**.

   Under **Microsoft APIs** group, select **Microsoft Graph API** option.

   Select **Application Permissions** and under **DeviceManagementManagedDevices** group, **select DeviceManagementManagedDevices.Read.All** checbox.



You are editing permission(s) to your application, users will have to consent even if they've alread

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as p all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services: Allow validated users to read and write protected content

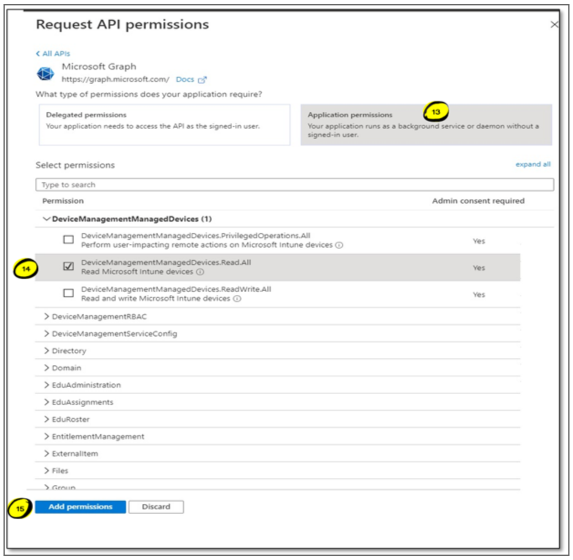
Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central

Intune: Programmatic access to Intune data

Office 365 Management APIs: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

SharePoint: Interact remotely with SharePoint data



What type of permissions does your application require?

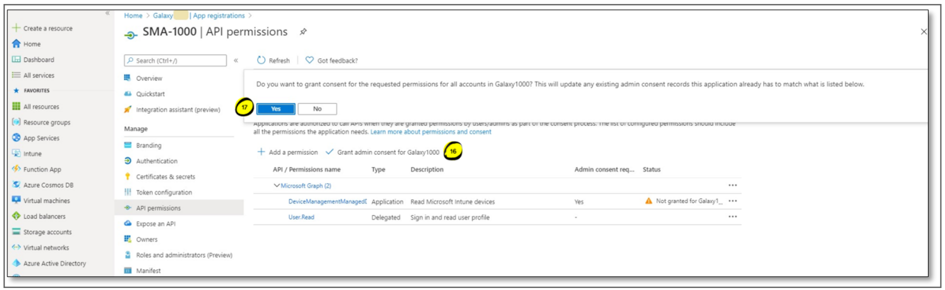
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Permission	Admin consent required
DeviceManagementManagedDevices (1)	
□ DeviceManagementManagedDevices.PrivilegedOperations.All Perform user-impacting remote actions on Microsoft Intune devices	Yes
☑ DeviceManagementManagedDevices.Read.All Read Microsoft Intune devices	Yes
□ DeviceManagementManagedDevices.ReadWrite.All Read and write Microsoft Intune devices	Yes
› DeviceManagementRBAC	
› DeviceManagementServiceConfig	
› Directory	
› Domain	
› EduAdministration	
› EduAssignments	
› EduRoster	
› EntitlementManagement	
› ExternalItem	
› Files	
› Group	

6. Click **Add Permission.**

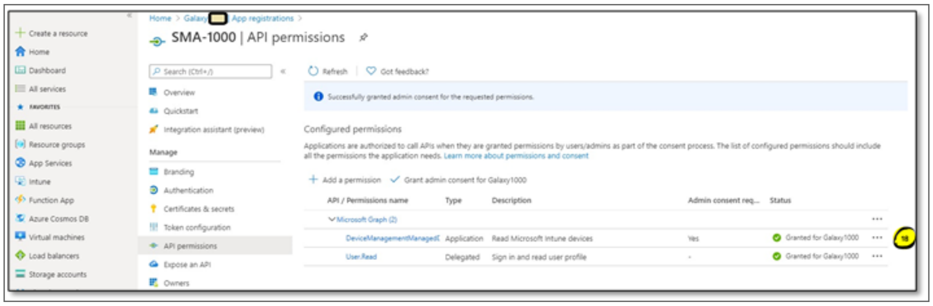
7. Once permission is added, select and add consent for the permission as shown below:



Do you want to grant consent for the requested permissions for all accounts in Galaxy1000? This will update any existing admin consent records this application already has to match what is listed below.

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
DeviceManagementManaged[	Application	Read Microsoft Intune devices	Yes	Not granted for Galaxy1...
User.Read	Delegated	Sign in and read user profile	-	



Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
DeviceManagementManaged[	Application	Read Microsoft Intune devices	Yes	Granted for Galaxy1000
User.Read	Delegated	Sign in and read user profile	-	Granted for Galaxy1000

ⓘ **NOTE:** Ensure to register **Application (Client ID)**, **Object ID** and **Directory (Tenant ID)** in Azure portal.

8. To create a **Client Secret** key do the following:

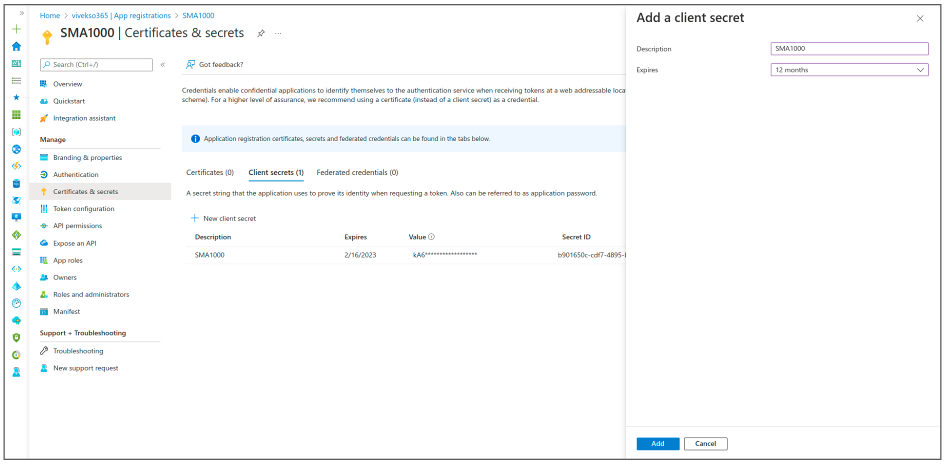
   a. In Azure portal go to **Manage**>**Certificates &Secrets**> **Client**.

   b. Click to add new client secret.

   c. In the **Add a client secret** dialog box add the description and select the expire time.

d. Click **Add**.

e. Click the and copy the **Value** to paste in the **Client secret** field in AMC. For more information refer to the Configuring Microsoft Intune in AMC section.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable loca scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
SMA1000	2/16/2023	kA6******************	b901650c-cdf7-4895-l

Add a client secret

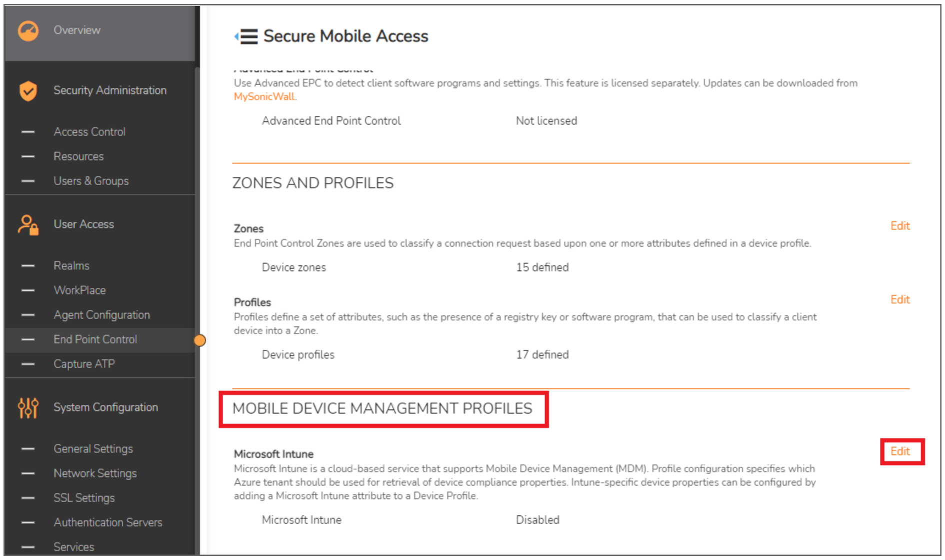
Description: SMA1000

Expires: 12 months

Configuring Microsoft Intune in AMC

To configure Microsoft Intune in AMC:

1. Log in to AMC.
2. Navigate to **User Access > End Point Control > Mobile Device Management Profiles**.



Use Advanced EPC to detect client software programs and settings. This feature is licensed separately. Updates can be downloaded from MySonicWall.

Advanced End Point Control Not licensed

ZONES AND PROFILES

Zones

End Point Control Zones are used to classify a connection request based upon one or more attributes defined in a device profile.

Device zones 15 defined

Profiles

Profiles define a set of attributes, such as the presence of a registry key or software program, that can be used to classify a client device into a Zone.

Device profiles 17 defined

MOBILE DEVICE MANAGEMENT PROFILES

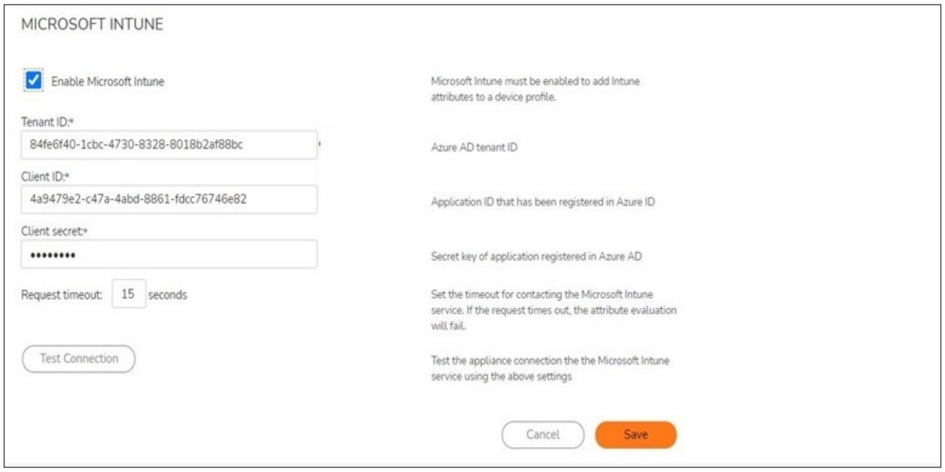
Microsoft Intune

Microsoft Intune is a cloud-based service that supports Mobile Device Management (MDM). Profile configuration specifies which Azure tenant should be used for retrieval of device compliance properties. Intune-specific device properties can be configured by adding a Microsoft Intune attribute to a Device Profile.

Microsoft Intune Disabled

3. Click **Edit**.

The following screen appears.



MICROSOFT INTUNE

☑ Enable Microsoft Intune — Microsoft Intune must be enabled to add Intune attributes to a device profile.

Tenant ID:* 84fe6f40-1cbc-4730-8328-8018b2af88bc — Azure AD tenant ID

Client ID:* 4a9479e2-c47a-4abd-8861-fdcc76746e82 — Application ID that has been registered in Azure ID

Client secret:* •••••••• — Secret key of application registered in Azure AD

Request timeout: 15 seconds — Set the timeout for contacting the Microsoft Intune service. If the request times out, the attribute evaluation will fail.

Test the appliance connection the the Microsoft Intune service using the above settings

4. In the **Intune MDM Settings** screen;
   a. Select **Enable Microsoft Intune** check box.
   b. In the **Tenant ID** (**Directory**) field, enter Azure tenant ID.
   c. In the **Client ID** (**Application**) field, enter the Application ID that has been registered in Azure ID.
   d. In the **Client secret** field, enter the **Value** registered in Azure ID.

      ⓘ | **NOTE:** All the above fields are mandatory.

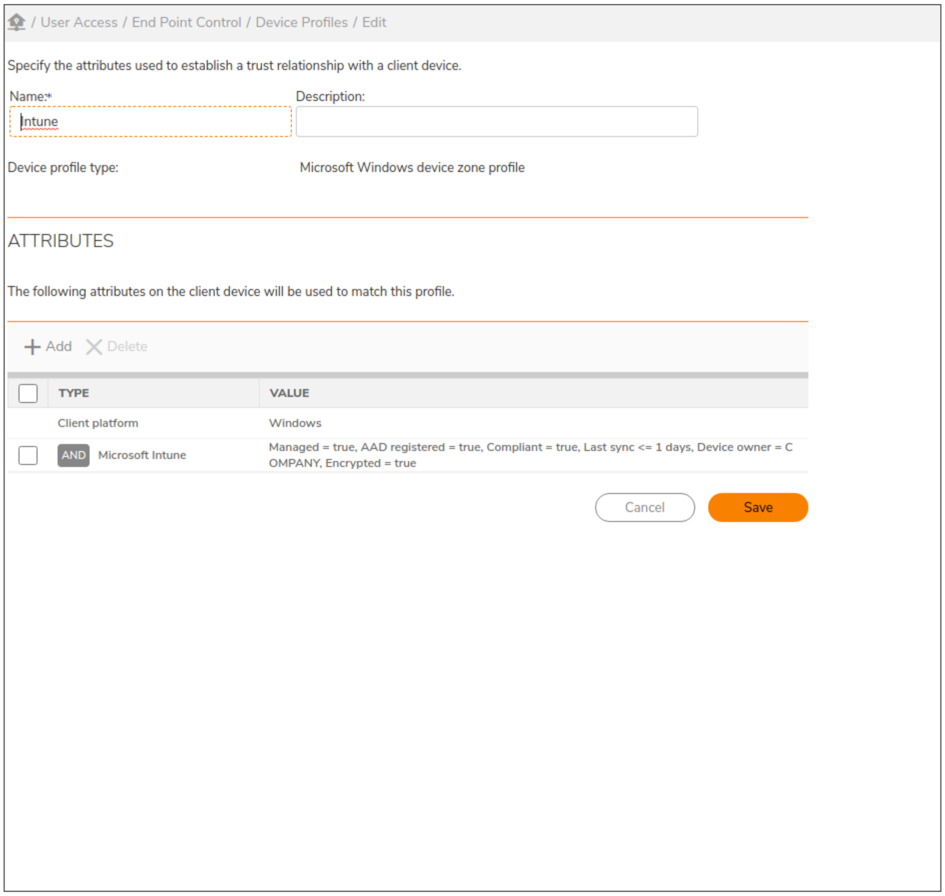
      ⓘ | **TIP:** The above information are generated while configuring Microsoft Intune in Azure. For more details, refer to the Configuring Microsoft Intune section.
   e. In the **Request timeout** field, set the timeout period for contacting the Microsoft Intune service. If the request times out, the attribute evaluation fails. The default request timeout period is 15 seconds.
5. Click **Test Connection** and **Save**.

Creating Windows Profile with Intune Attributes

To create Windows profile:

1. Log in to AMC.
2. Navigate to **User Access > End Point Control > Zones and Profiles > Profiles > Edit**.
3. In the **Profiles** tab, click **+** icon and select **Windows** to create a windows device profile.

4. Enter the name and description for the profile.



/ User Access / End Point Control / Device Profiles / Edit

Specify the attributes used to establish a trust relationship with a client device.

Name:* Intune

Description:

Device profile type: Microsoft Windows device zone profile

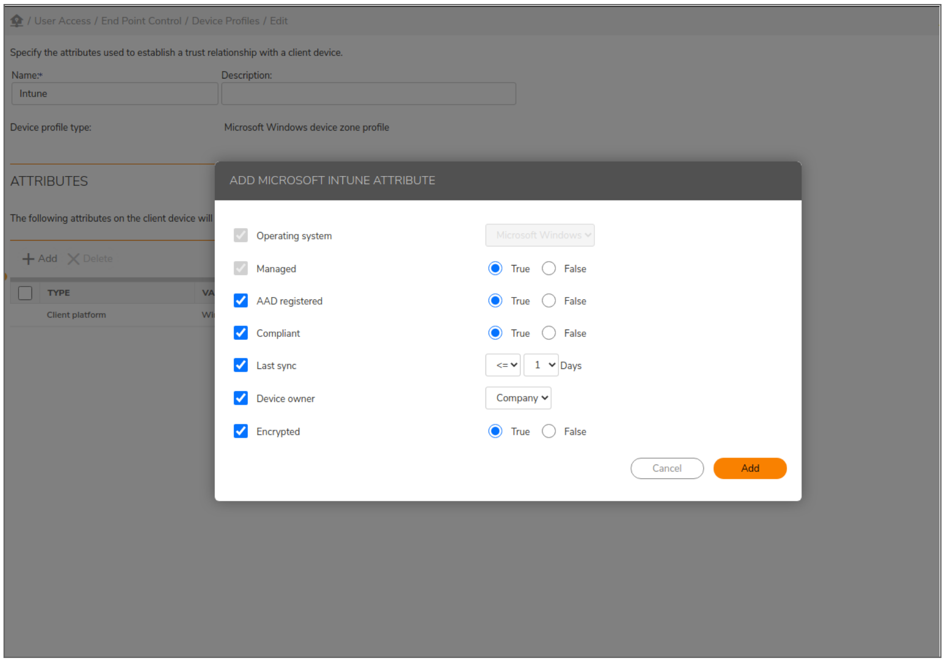
ATTRIBUTES

The following attributes on the client device will be used to match this profile.

□	TYPE	VALUE
	Client platform	Windows
□	AND Microsoft Intune	Managed = true, AAD registered = true, Compliant = true, Last sync <= 1 days, Device owner = COMPANY, Encrypted = true

5. Under **Attributes** , click **Add** .

6. Set values for **Managed**, **AAD registered**, **Compliant**, **Last sync**, **Device owner**, and **Encrypted** fields based on your requirements.



/ User Access / End Point Control / Device Profiles / Edit

Specify the attributes used to establish a trust relationship with a client device.

Name:* Intune

Description:

Device profile type: Microsoft Windows device zone profile

ATTRIBUTES

The following attributes on the client device will

□	TYPE	VA
	Client platform	Wi

ADD MICROSOFT INTUNE ATTRIBUTE

☑ Operating system — Microsoft Windows

☑ Managed — ● True ○ False

☑ AAD registered — ● True ○ False

☑ Compliant — ● True ○ False

☑ Last sync — <= 1 Days

☑ Device owner — Company

☑ Encrypted — ● True ○ False

7. Once configuration is complete, click **Add**.

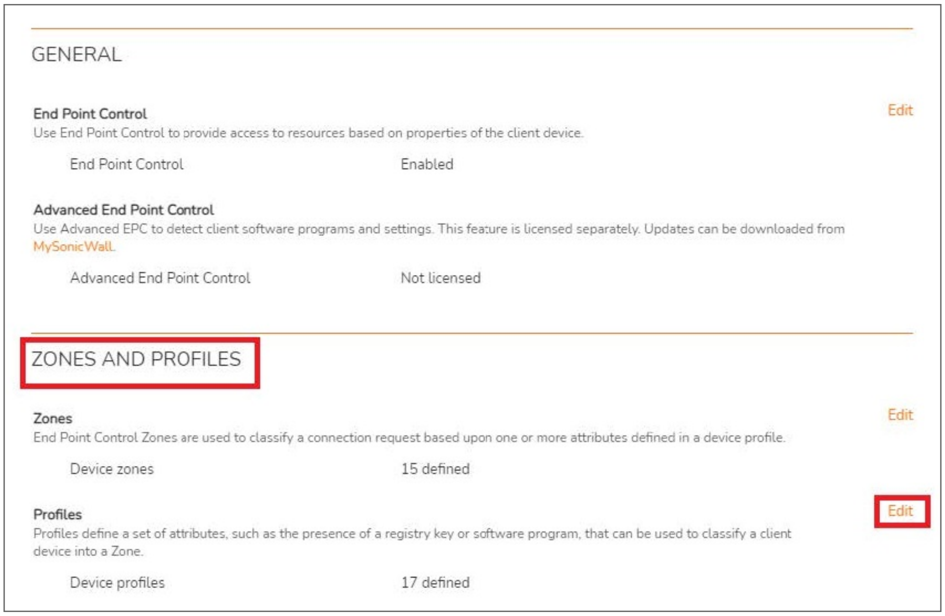
   All the attributes are added to the Profile.

8. In the AMC, add the created profile to a Zone and associate it to a Realm.

Creating Mac Profile with Intune Attributes

To create Mac profile:

1. Log in to AMC.
2. Navigate to **User Access** > **End Point Control** > **Zones and Profiles** > **Profiles** > **Edit**.



GENERAL

End Point Control
Use End Point Control to provide access to resources based on properties of the client device.

End Point Control	Enabled

Advanced End Point Control
Use Advanced EPC to detect client software programs and settings. This feature is licensed separately. Updates can be downloaded from MySonicWall.

Advanced End Point Control	Not licensed

ZONES AND PROFILES

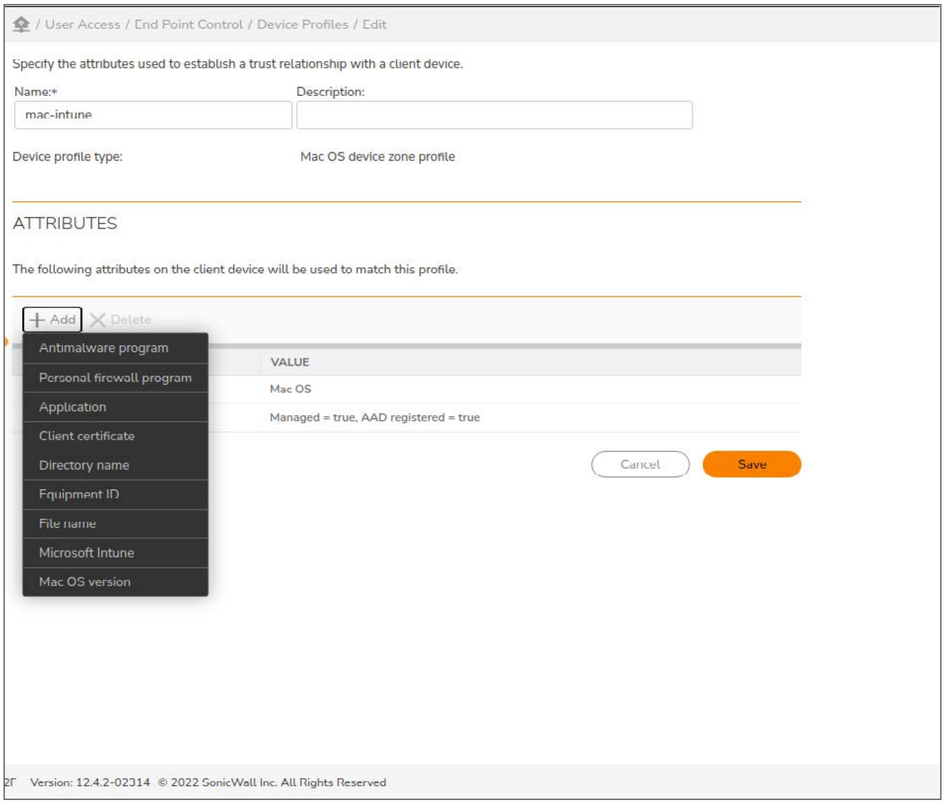
Zones
End Point Control Zones are used to classify a connection request based upon one or more attributes defined in a device profile.

Device zones	15 defined

Profiles
Profiles define a set of attributes, such as the presence of a registry key or software program, that can be used to classify a client device into a Zone.

Device profiles	17 defined

3. In the **Profiles** tab, click + icon and select **macOS** to create a mac device profile.
4. Enter the name and description for the profile.
5. Under **Add Attributes** group, click **+ Add** drop-down and select **Microsoft Intune**.



/ User Access / End Point Control / Device Profiles / Edit

Specify the attributes used to establish a trust relationship with a client device.

Name:* mac-intune

Description:

Device profile type: Mac OS device zone profile

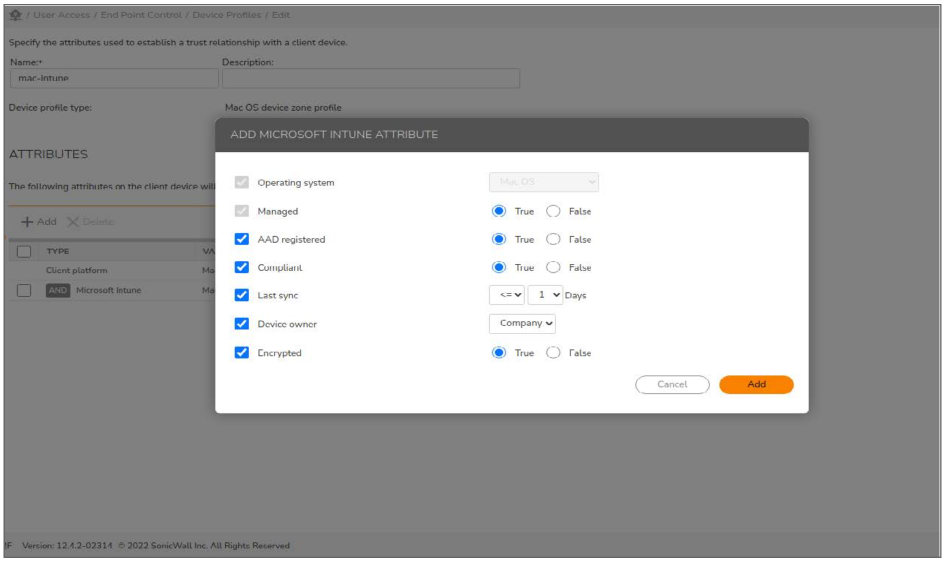
ATTRIBUTES

The following attributes on the client device will be used to match this profile.

VALUE
Mac OS
Managed = true, AAD registered = true

Version: 12.4.2-02314 © 2022 SonicWall Inc. All Rights Reserved

6. Set values for **Managed**, **AAD registered**, **Compliant**, **Last sync**, **Device owner**, and **Encrypted** fields based on your requirements.



/ User Access / End Point Control / Device Profiles / Edit

Specify the attributes used to establish a trust relationship with a client device.

Name:* mac-intune

Description:

Device profile type: Mac OS device zone profile

ATTRIBUTES

The following attributes on the client device will

	TYPE	VA
	Client platform	Ma
□	AND Microsoft Intune	Ma

ADD MICROSOFT INTUNE ATTRIBUTE

☑ Operating system	Mac OS
☑ Managed	● True ○ False
☑ AAD registered	● True ○ False
☑ Compliant	● True ○ False
☑ Last sync	<= 1 Days
☑ Device owner	Company
☑ Encrypted	● True ○ False

Version: 12.4.2-02314 © 2022 SonicWall Inc. All Rights Reserved

7. Once configuration is complete, click **Add**.

   Attribute is added to the current profile with all the configured fields.

8. In the AMC, add the created profile to a Zone and associate it to a Realm.

Configuring MSIntune in Client

1. Ensure the testing client is enrolled to Intune under same Azure directory where application is registered.
2. For MAC enrollment process, refer to the following Microsoft support documents.
   - https://docs.microsoft.com/en-us/mem/intune/enrollment/macos-enroll
   - https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-your-device-in-intune-macos-cp

   Or

   For windows enrollment process, refer to the following Microsoft support documents.
   - https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device
   - https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods
3. Install Connect Tunnel or log in from extra web to Intune Configured Realm.

   After successful login, if Intune profile conditions are satisfied, it should classify to Intune zone else it falls back to default or quarantine zone.

Creating Zones for Special Situations

While the majority of connection requests—those involving Microsoft Windows and Edge, Google Chrome, or Mozilla Firefox—can be accommodated by device zone configurations, you may need to address special situations involving other operating systems and browsers, or connection requests that don't match any of the zones you've defined. You can use zones and device profiles to address the following types of situations:

- Clients that don't match the criteria for any defined zones and device profiles.
- Clients that don't support the EPC interrogation necessary for classifying a client into an EPC zone.
- Clients running certain Web browsers (anything other than Microsoft Edge, Google Chrome, and Firefox) on Windows, and Safari on macOS.
- Special classes of users who require access regardless of the client device they're running.

Be sure to configure the global **Default** zone, which is implicitly present in every community configured in AMC

Topics:

- Defining Zones for Non-Standard Browsers
- Collecting Equipment IDs from Unregistered Devices
- Defining Zones for Special Classes of Users

Defining Zones for Non-Standard Browsers

When a user connects to the SMA appliance, the appliance interrogates the user's computer and determines (among other things) what operating system it's running and what Web browser is in use. EPC works on all supported OS and browsers supported by SMA and also with Connect Tunnel client as well. This prevents them from being placed in the Default zone, which might block their access. The only attribute used to distinguish this type of zone is the presence of the Windows system.

To define a zone for clients with non-standard browsers:

1. In the AMC, navigate to **User Access > End Point Control**.
   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.
   The **Zones and Profiles** page displays.
3. Click the **+** (New) icon.
4. Select **Windows** from the menu.
   The **Add Device Profile** page displays.
5. In the **Name** field, type a meaningful name for the device profile.
6. In the **Description** field, type a descriptive comment about the device profile.
7. In the **Add attribute** area:
   a. Select **Windows version** from the **Type** list and enter the appropriate values.
   b. Click **Add to current attributes**. Do not specify any other attribute settings.
8. Click **Save**.
9. Select the check box for the browser **Device profile** that you want to include in the zone.

10. Use the checkmark to move the items to the **In use** list.

11. Click **Save**.

Collecting Equipment IDs from Unregistered Devices

Every device has a unique identifier, and you can use this identity in a device profile to ensure that only certain devices have access to protected resources. But before you can add equipment ID data to your directory server as a user attribute, you must first collect the data. You can do this in several ways:

- By creating device profiles for unregistered devices and having users log in: the device ID is collected in the `Unregistered device log`. See Creating Device Profiles that Allow Unregistered Devices.
- By creating a device profile that uses a device identity, but does not have the **Match Profile if user has no registered devices** option enabled. See Disabling Match Profile if User has no Registered Devices in the Device Profile.
- By creating a quarantine zone associated with a device profile that matches users who log in using an unregistered device. See Quarantining Unregistered Devices.
- By creating a deny zone associated with a device profile that matches users who log in using an unregistered device. See Locking Out Unregistered Devices.
- By exporting the log messages for login attempts by unregistered devices to an external machine, where an IT administrator can view the list and register the devices or they can be automatically registered. See Exporting the Unregistered Device Log for External Processing.

NOTE: When selected, the **Match profile if user has no registered devices** check box is applicable when the user has no devices registered in the back end AD or LDAP server and there are no hard coded devices in the device profile.

For example, consider the case where two attributes have been created for user test in the AD/LDAP server, and these attributes are mapped to two policy variables. A device profile is created containing these two variables and the equipment ID *4JV5DQH1*. The check box is selected. This device profile is a part of a zone called *std_desc*. Unlike user *test*, user *test1* has no representation in the backend LDAP/AD server.

User *test* logs in with a device that is registered in the backend server. The zone classification is *std_desc*. However, user *test1* logs in with the same device and is classified into the default zone. The check box does not apply to user *test1* in this case.

However, if you remove the device ID *4JV5DQH1* from the device profile, leaving just the two policy variables, you will see a different zone classification for user *test1*. In this case, user test logs in with a registered device and is classified into the *std_desc* zone. User test1 logs in and is also classified into the *std_desc* zone. The checkbox applies in this case because user *test1* has no devices registered, the two policy variables in the device profile of the zone return with NULL values, and there isn't the third hard-coded device in the device profile.

If you are using mobile devices, you may already have the device identities entered into your database. In this case, you could simply refer to them in a profile. Users logging in from one of these devices will match this profile and qualify for the associated zone.

The device identifier is usually an attribute in the authentication directory represented by a variable; for example, `{device_identity}`. The format of the identifier differs, depending on the kind of device used:

- For a Microsoft Windows device, the identifier is a unique hard-drive serial number; for example, *WD-WMAM9SK79685*.
- For a macOS device, the Universal Unique Identifier (UUID) is used. A UUID is a 128-bit number that combines references to the network address of the host that generated the UUID, the timestamp, and a random number. An example of a UUID is: *951A240E-F502-5632-BDAB-D1ECA43FA371*.
- For a Linux device, the UUID is the device identifier.
- For a Virtual Machine, the UUID is the device identifier.
- For a Google Android device, the device serial number is the identifier.
- For an Apple iPhone/iPad, the device serial number is the identifier.
- In the case of the Apple iPhone, the device prepends `Appl` to its device ID/serial number when it communicates with Exchange servers. For example: *Appl828315FLY7H*.

Another method to get the correct device ID for a smart phone is to view the POST message in the AMC log after the phone attempts to connect to the appliance. Navigate to the **Logging** page, and select *Web proxy audit log* in the **Log file** drop-down menu on the **View Logs** tab. The POST message looks like this:

```
http://10.10.11.12/Microsoft-Server-
ActiveSync?User=jt&DeviceId=Appl828315FLY7H&DeviceType=iPh one&Cmd=Sync
```

Use the DeviceId value in your database for profiles to refer to.

Your directory server may be set up with a different attribute for each of these types of identifiers, or you can store the data in a single attribute. In this example, a single attribute and variable is used.

Creating Device Profiles that Allow Unregistered Devices

To collect equipment IDs from unregistered devices by using a device identity variable with device profiles:

1. Identify or set up the AD or LDAP authentication server and realm you want users with unregistered devices to log in to. If you're starting from scratch, see Creating Realms for more information. In this example, the realm is named *Employees*.
2. Create a variable named *device_identity* that points to an attribute in the directory server specified in *Step 1* (you can create the variable and capture data even if the attribute it points to doesn't exist yet):
    a. In the AMC, navigate to **Security Administration > Resources**.
    b. Click on the **Variables** tab.
    c. Click the **+** (New) icon.
    d. In the **Name** field, enter the name for the variable; for example, `device_identity`.
    e. Select **User attribute** from the **Type** list, and then make sure **Employees** is selected in the **Realm** list.
    f. If the user attribute that holds device ID data already exists, enter a valid user name in the **User** field, and then select the attribute from the **Attribute** list. If it doesn't exist yet, just enter its name in the **Attribute** field.

g. If it’s possible that some users will be associated with more than one device (for example, a desktop computer and a laptop), select **Multiple results** in the **Output** list.

3. Now create device profiles and a zone for unregistered devices. If you are collecting data from all three types of devices, you’ll need one device profile for each one:

   a. In the AMC, navigate to **User Access > End Point Control**.

      The **End Point Control** page displays.

   b. Make sure that End Point Control is enabled.

   c. In the **Zones and Profiles** section, click **Edit** next to **Profiles**.

      The **Zones and Profiles** page displays.

   d. Click the **+** (New) icon.

   e. Select the platform for which you want to create the new device profile.

   f. Give the device profile a name (for example, Unregistered - Windows), and then select **Equipment ID** in the attribute **Type** list.

   g. Select **Matches** as the **Value**. You’ll create a Standard zone later in this procedure.

   h. Click the **{variable}** button next to the **Device identifier** field, select the variable you created in step 2, and then click **Insert**. Click **{variable}** again to close the list.

   i. In the **Unregistered devices** area, select the **Match profile if user has no registered devices** check box. Devices that are not already registered on the external AD/LDAP server will be a match for this profile and their identifiers will be recorded in the *Unregistered device log*. If you haven't already defined the variable, you'll see a warning (*Undefined: {device_identity}*), which can be ignored for now.

   j. Click the **Add to Current Attributes** button, and then click **Save**.

   k. Add a device profile for each of the other types of devices you want to accommodate. For example, Unregistered - WinMobile, or Unregistered - ActiveSync.

4. Create a Standard zone named *Data collection* that uses the device profiles that you created. See Creating a Device Zone for more information.

5. Now create a community named *New devices* in the *Employees* realm. On the **End Point Control Restrictions** page for that community, move the *Data collection* zone to the **In use** list. See Creating and Configuring Communities if you need help setting up a community.

6. When you apply and save your changes, click **End Point Control** in the main navigation menu.

7. When an unregistered device is detected during login, the user is placed in the *Data collection* zone because the device matches the *Unregistered* profile. To see device identity details, select **Unregistered device log** on the **Logging** page in AMC.

8. Select **No devices** in the **Device count** list, and then click **Refresh**, so that you're sure to capture all new users.

9. If you need to do any additional analysis of the logged data, export it to an XML file. You can reduce the size of the exported file by first applying filter or search criteria. The **Show last <n>** messages setting determines the maximum number of messages included in the exported log file.

Disabling Match Profile if User has no Registered Devices in the Device Profile

If you create a device profile that uses a device identity and disable the **Match Profile if user has no registered devices** option, a user with a new device (even if some devices are registered to that user) will not match this profile and will not be qualified into this zone. The unregistered device ID will be collected and placed into the unregistered devices list, provided that the user met all other (non-device) criteria to match the profile. The administrator can collect the device information from the unregistered device list and then register the device semi-automatically. Thus, with no user interaction, the next time the user attempts to log in using the device they may be able to classify into the zone.

Topics:

- Quarantining Unregistered Devices
- Locking Out Unregistered Devices
- Exporting the Unregistered Device Log for External Processing

Quarantining Unregistered Devices

You can create a device profile that specifies that the user does not match any of the device IDs currently registered for this user. A user with a new device will match this profile and be placed into the quarantine zone. You can configure a message to the user that the current device is unregistered, but that the device information was collected from their login attempt and their device will be registered for them, allowing their next login to qualify for the usual (non-quarantine) zone.

Locking Out Unregistered Devices

You can use a deny zone to lock out a particular device. To do this, create a device profile that contains an Equipment ID attribute and select the **Does not match** check box when adding the Device Identifier. This feature allows you to lock out, for example, a device that you suspect has been compromised, while not completely locking out the user who owns that device. The device information is collected from the login attempt.

Exporting the Unregistered Device Log for External Processing

There are unregistered device log messages for every new unregistered device that is used in a login attempt. These messages can be exported in XML format to an external machine either from the **Logging** page in the AMC or by using a *curl* or *wget* command from an external machine. See Unregistered Device Log Messages for more information. This export feature allows you to collect these messages and then either automatically register each device, or inform a help desk of each new unregistered device that was used by each user.

- **Advanced**: If you need be notified immediately when a user attempts to log in using an unregistered device, you can configure a Syslog server on the Configure Logging page in AMC. The appliance will generate a log message with the following format when a login or login attempt occurs:
- **New Equipment**: user '#1', platform '#2', device '#3', existing Devices '#4' where:

- #1 is the name of the user
- #2 is the name of the platform
- #3 is the ID of this device or piece of user equipment
- #4 is the number of devices already registered for this user

Defining Zones for Special Classes of Users

Another method for preventing special classes of trusted users from being assigned to the **Default** zone (and potentially being denied access) involves creating a zone that contains no device profiles, and then assigning that zone to a community to which only those trusted users belong.

For example, if you want system administrators to be able to access network resources regardless of the client device they're using, you could assign them to a community that contains a no-profile zone. Then when system administrators select a realm that references that community and log in, they are placed in the no-profile zone, instead of the global **Default** zone, which may be set up to block unrecognized clients.

To create a no-profile zone:

1. In the AMC, navigate to **User Access > End Point Control**.
   The **End Point Control** page displays.
2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.
   The **Zones and Profiles** page displays.
3. Click the **+** (New) icon.
4. Select the zone to create
5. In the **Name** field, type a meaningful name for the zone.
6. In the **Description** field, type a descriptive comment about the zone.
7. You can optionally select a **Required data protection tool** for the zone. However, if you want this special class of trusted users to have flexibility regarding the types of devices they're connecting with, leave this field set to **None**.
8. Click **Save**.

After you've defined the no-profile zone, you must create a realm specifically for this special class of trusted users. Configure the realm with a dedicated community so that only this special class can log in to it. For more information, see Assigning Members to a Community.

Using End Point Control Agents

Use End Point Control Agents to perform common EPC tasks such as enabling or disabling the virtual keyboard.

End Point Control Tasks

Item	Description
Enable virtual keyboard	Enables the virtual keyboard.

Require use of keyboard	To select the use of keyboard.

Using the Virtual Keyboard to Enter Credentials

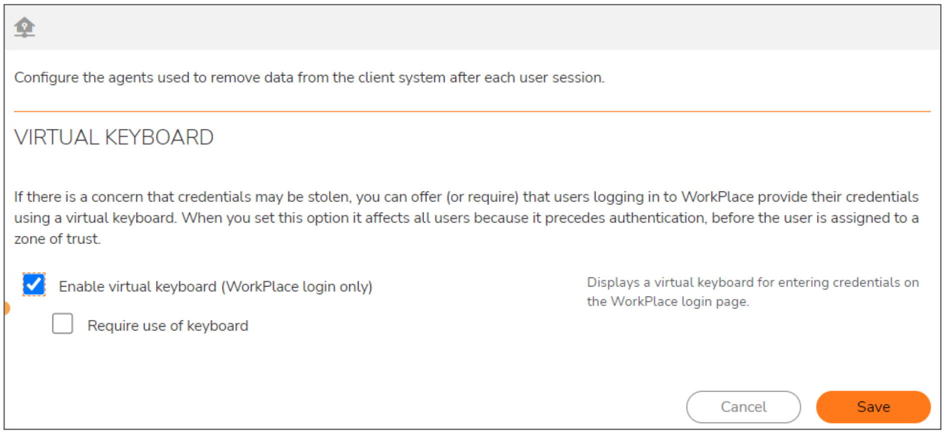
If there is a concern that credentials may be stolen, you can offer (or require) that users logging in to WorkPlace provide their credentials by pointing to characters on a keyboard display instead of typing them.

Because the virtual keyboard is used before a user is authenticated (and before a realm is chosen), the way in which it's configured applies to all realms: you can't offer the virtual keyboard to just certain groups of users, or require it only in certain cases. End Point Control does not have to be enabled in order for the virtual keyboard to be used.

The virtual keyboard settings do not apply to small form factor devices, such as smart phones; for information about optimizing WorkPlace for these devices, see Optimizing WorkPlace for Display on Small Form Factor Devices .

To configure the virtual keyboard in WorkPlace:

1. In the AMC, navigate to **User Access > End Point Control**.
   The **End Point Control** page displays.
2. In the **End Point Control agents** section, click **Edit**.
   The **End Point Control Agents** page displays.



Configure the agents used to remove data from the client system after each user session.

VIRTUAL KEYBOARD

If there is a concern that credentials may be stolen, you can offer (or require) that users logging in to WorkPlace provide their credentials using a virtual keyboard. When you set this option it affects all users because it precedes authentication, before the user is assigned to a zone of trust.

☑ Enable virtual keyboard (WorkPlace login only) — Displays a virtual keyboard for entering credentials on the WorkPlace login page.

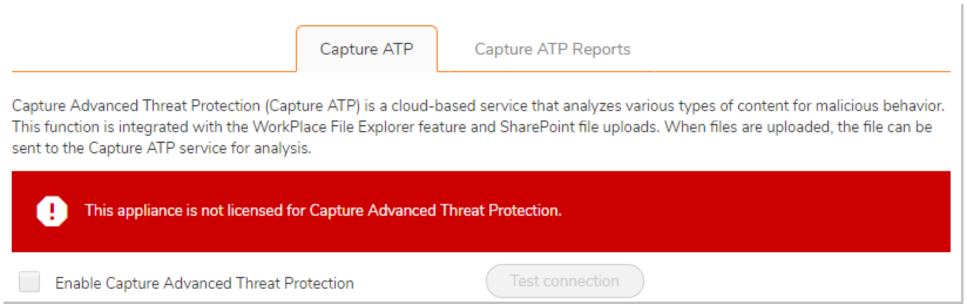
□ Require use of keyboard

3. Check **Enable virtual keyboard (Workplace login only)** check box to let users enter WorkPlace login credentials using a virtual keyboard, which reduces the risk of credentials being stolen. When this setting is enabled, all WorkPlace users, regardless of login realm, have this option.
4. If the virtual keyboard is enabled, check the **Require use of keyboard** check box to require users to use a virtual keyboard to enter their WorkPlace login credentials.
5. Click **Save**.

Capture Advanced Threat Protection

Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that analyzes various types of content for malicious behavior. This function is integrated with the WorkPlace File Explorer feature and SharePoint web service. When files are uploaded, the file can be sent to the Capture ATP service for analysis.

> ⓘ **IMPORTANT:** Capture Advanced Threat Protection (Capture ATP) is an add-on security service to the firewall that helps a firewall identify whether a file is malicious.
>
> Before you can enable Capture ATP you must first get a license. If the Capture ATP license has not been activated, an error message displays:



Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that analyzes various types of content for malicious behavior. This function is integrated with the WorkPlace File Explorer feature and SharePoint file uploads. When files are uploaded, the file can be sent to the Capture ATP service for analysis.

This appliance is not licensed for Capture Advanced Threat Protection.

□ Enable Capture Advanced Threat Protection

> After Capture ATP is licensed, you can view Capture ATP status in your MySonicWall account as well as configure and receive alerts and notifications.
>
> For further information about Capture ATP, licensing it, and using your MySonicWall account to configure and receive alerts and notifications, see the *Capture Advanced Threat Protection Feature Guide*.

Topics:

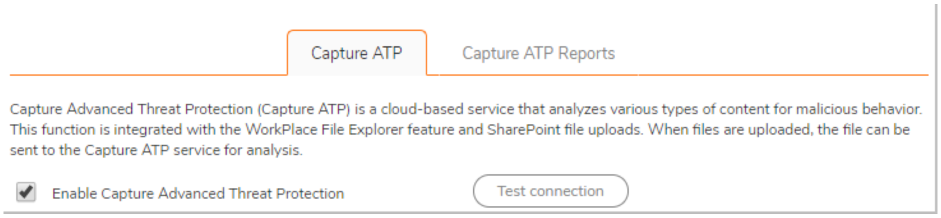
- Enabling Capture ATP
- Web Services
- Advanced Settings

Enabling Capture ATP

After being successfully licensed, Capture ATP must be enabled before it will begin analyzing files for malicious behavior.

To enable Capture ATP:

1. In the AMC, navigate to **User Access > Capture ATP**.
2. On the **Capture ATP** page, select **Enable Capture Advanced Threat Protection**.



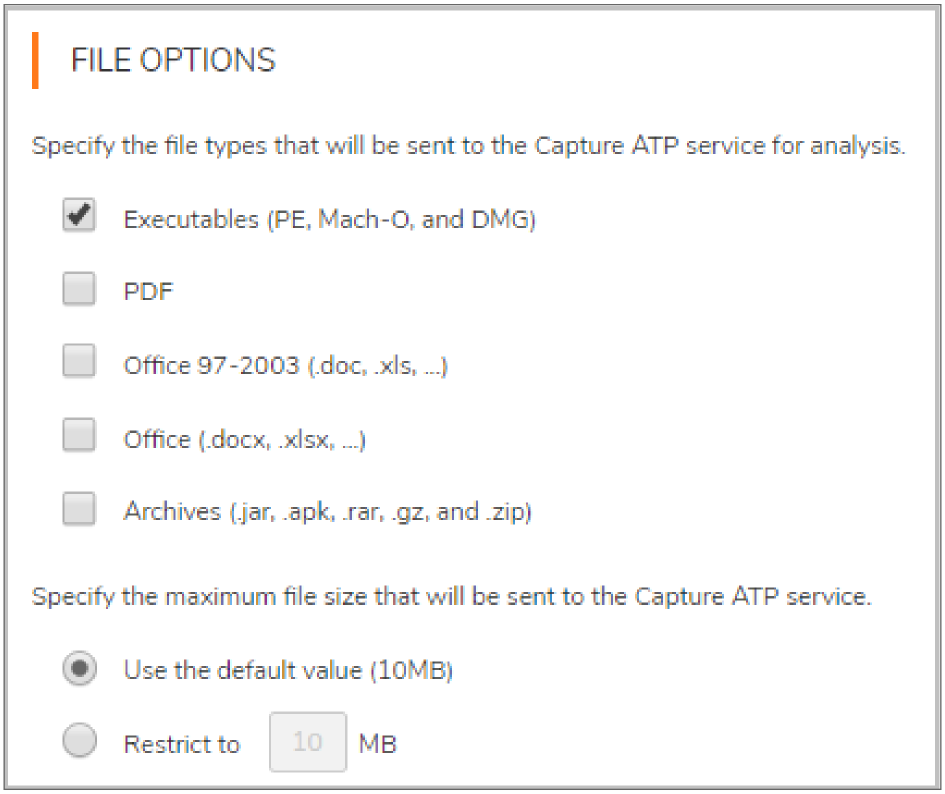
Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that analyzes various types of content for malicious behavior. This function is integrated with the WorkPlace File Explorer feature and SharePoint file uploads. When files are uploaded, the file can be sent to the Capture ATP service for analysis.

☑ Enable Capture Advanced Threat Protection

3. To verify the connection to the Capture ATP service, click the **Test connection** button.

File Options

The **File Options** settings allow you to specify which file types will be sent to the Capture ATP service for analysis and the maximum size of those files.



FILE OPTIONS

Specify the file types that will be sent to the Capture ATP service for analysis.

- ☑ Executables (PE, Mach-O, and DMG)
- ☐ PDF
- ☐ Office 97-2003 (.doc, .xls, ...)
- ☐ Office (.docx, .xlsx, ...)
- ☐ Archives (.jar, .apk, .rar, .gz, and .zip)

Specify the maximum file size that will be sent to the Capture ATP service.

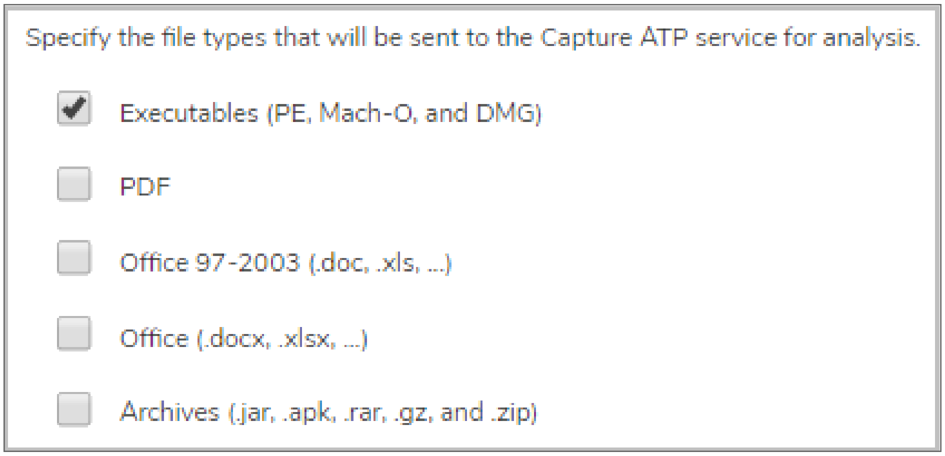
- ● Use the default value (10MB)
- ○ Restrict to 10 MB

Topics:

- Setting the File Types
- Setting the Maximum File Size

Setting the File Types

You can select the types of files to be submitted to Capture ATP for inspection.



Specify the file types that will be sent to the Capture ATP service for analysis.

☑ Executables (PE, Mach-O, and DMG)

□ PDF

□ Office 97-2003 (.doc, .xls, ...)

□ Office (.docx, .xlsx, ...)

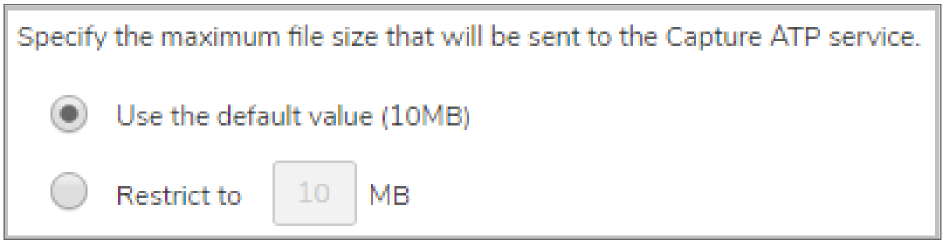
□ Archives (.jar, .apk, .rar, .gz, and .zip)

To set which file types are analyzed:

1. From the appliance management console, navigate to **User Access > Capture ATP**.
2. In the **File Options** section, select the file types you want analyzed by the Capture ATP service. By default, only the **Executables (PE, Mach-O, and DMG)** file type is enabled.
3. Click the **Save** button.

Setting the Maximum File Size

You can select the maximum size of files to be submitted to Capture ATP for inspection.



Specify the maximum file size that will be sent to the Capture ATP service.

● Use the default value (10MB)

○ Restrict to 10 MB

To set the maximum file size:

1. In the AMC, navigate to **User Access > Capture ATP**.
2. In the **File Options** section, choose one of the options.
   - Select **Use the default value (10MB)** to use the default file size of 10MB.
   - **Restrict to __ MB** to specify your own maximum file size.

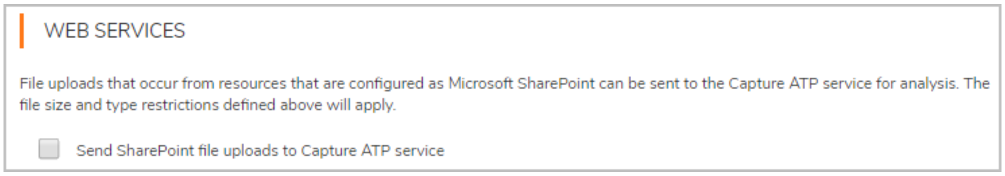
NOTE: The maximum file size supported by Secure Mobile Access 12.4 is 50MB.

3. Click the **Save** button.

Web Services

NOTE: The resource must be classified as a SharePoint web service for this feature to function. For instructions to configure SharePoint as a web service, refer to Configuring a Resource as a SharePoint Web Service.

Files uploaded to your SharePoint sites can be sent to Capture ATP for inspection.



WEB SERVICES

File uploads that occur from resources that are configured as Microsoft SharePoint can be sent to the Capture ATP service for analysis. The file size and type restrictions defined above will apply.

□ Send SharePoint file uploads to Capture ATP service

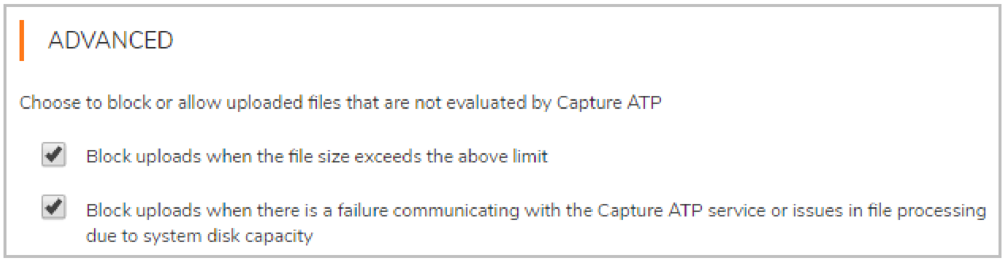
To configure Capture ATP to analyze files uploaded to SharePoint sites:

1. In the AMC, navigate to **User Access > Capture ATP**.
2. In the **Web Services** section, select **Send SharePoint file uploads to Capture ATP service**.
3. Click the **Save** button.

NOTE: The restrictions set for Capture ATP for file types and maximum sizes will apply to files uploaded to SharePoint site. See Setting the File Types and Setting the Maximum File Size for more information on configuring these options.

Advanced Settings

The **Advanced** settings allows you to choose to block or allow uploaded files that are not evaluated by Capture ATP.



ADVANCED

Choose to block or allow uploaded files that are not evaluated by Capture ATP

☑ Block uploads when the file size exceeds the above limit

☑ Block uploads when there is a failure communicating with the Capture ATP service or issues in file processing due to system disk capacity

- Select **Block uploads when the file size exceeds the above limit** to stop files from being uploaded that exceed the maximum file size specified in the **File Options** section. (This is selected by default.)
- Select **Block uploads when there is a failure communicating with the Capture ATP service or issues in file processing due to system disk capacity** to stop files from being uploaded when the

appliance cannot communicate with the Capture ATP service or when the performance of the appliance is impacted by high disk usage.(This is selected by default.)

7

Components

Topics:

The WorkPlace Portal

A Quick Tour of WorkPlace

This section gives a general overview of WorkPlace from the customer perspective.

The WorkPlace portal provides your users with dynamically personalized access to Web-based (HTTP) resources. It also gives users access from their Web browsers to files and folders on Windows file servers, and to TCP/IP resources through Secure Mobile Access agents that can be provisioned from WorkPlace.

The SMA appliance includes a default WorkPlace portal that you can modify. Additional sites can be set up for different user populations, each with its own appearance; see WorkPlace Sites for more information. For details on client system requirements for WorkPlace, see System Requirements.

When users log into the browser address for WorkPlace, they will be presented with an Authentication Page. Users then log in to the **Authentication** page, using their Username and Password. This page also allows users the option of changing their password.

If users authenticating with a client certificate do not see this page, in lieu of the **Authentication** page, a one-time password may be required. The administrator sends an email containing the password, which is requested through this screen,

ⓘ **NOTE:** If you’ve configured the system to use End Point Control, see End Point Control and the User Experience for information on how it affects the way users access the system.

After supplying their authentication credentials, WorkPlace checks for a current licensing agreement. If there is a problem with licensing, a message appears, indicating this is a licensing failure and not some other kind of authentication failure, such as a mis-typed password. Users should contact their administrator.

Depending on how the system is configured, users may be required to agree to an Acceptable Use Policy or other licensing agreement.

The AUP may display specific messages or instructions the user needs to agree to. Users who do not accept the license agreement will not be able to access WorkPlace.

Topics:

- Home Page
- Intranet Address Field
- Bookmarks
- Custom RDP Bookmarks
- Network Explorer Page

Home Page

After a user has provided authentication, providing licensing is up-to-date, the WorkPlace home page displays. WorkPlace could include a personal bookmarks area, with relevant links to other resources. This area may contain pre-configured bookmarks from the administrator, or users can add their own links to resources or web sites.

Configurable WorkPlace Elements

Most of the features on the home page are configurable; see the below table.

Configurable WorkPlace Elements

WorkPlace element	Description
Layout	WorkPlace page content and layout can be customized on a per-community basis. These layout elements include: • Content (what shortcuts and shortcut groups are displayed) • Pages (single vs. multiple) • Columns (single vs. multiple) • Navigation (on the left or along the top) See Modifying the Appearance of WorkPlace for details.
Connect Tunnel	You can define custom connections for the Connect Tunnel client from the WorkPlace portal.

Help button	The Help system included with WorkPlace contains all the basic information that a user will need. If you would like to make a custom HTML help file available to users instead, you can specify it when you confiigure your WorkPlace style. This is a convenient way to add information that is unique to your environment (for example, information about the resources available on your VPN, and technical support details). This file must be a well-formed, single HTML file.
Shortcuts **Shortcut groups**	These are administrator-defined shortcuts to the Web, file system, and terminal server resources that the user is allowed to access. Shortcuts are dynamically displayed based on your access policy: each user sees only those resources he or she has privileges to use. Each type of shortcut behaves differently: • **Web resource**: Opens in a new browser window. • **Terminal server resource**: Opens in a new browser window and the appropriate graphical terminal agent is automatically started or, if necessary, provisioned. • **Shared folder or file**: Opens the WorkPlace Network Explorer page, which appears in a new browser window. Network shortcuts, which point to file system resources, do not appear if you have disabled all access to file system resources (disabling access to file system resources is described in Configuring WorkPlace General Settings). • **Bookmarks**: Provides all basic bookmark functionality (RDP, Citrix, VNC, Telnet, and SSHv2) of Workplace User defined bookmarks. • **Custom Shortcuts**: Behaves according to the custom configuration. For information about creating shortcuts, see Working with WorkPlace Shortcuts.

Built-In WorkPlace Elements

When you set up a WorkPlace portal for users, you can choose from among several built-in resources and WorkPlace elements; see the below table. If you offer these resources, they can be configured on a per-community basis.

Built-in WorkPlace Elements

WorkPlace element	Description

Intranet Address	You can specify whether you want this box to appear and configure whether it can be used to access Web resources (by typing a URL), file system resources (by typing a UNC path name), or both. See Intranet Address Field for details.
Personal Bookmarks	You can allow users to create and manage personal links (similar to bookmarks) that point to URLs and other resources, such as SMB hosts, protected by the SMA appliance. Personal links are stored on the appliance; users have access to them whenever they are logged in to WorkPlace, regardless of the computer they are using. See Bookmarks for more information.
Connect Tunnel	You can make the built-in **Install Connect Tunnel** shortcut available to enable users to download and install the Connect Tunnel client from the WorkPlace portal.
Network Explorer	You can offer users the ability to browse a Windows network containing shared folders and files. See Network Explorer Page for more information.

WorkPlace Status Bar

The WorkPlace pages have a status bar; see the WorkPlace status bar elements table.

WorkPlace Status Bar Elements

WorkPlace element	Description
Access	Indicates which user access methods are currently running. For more information about user access agents, see User Access Components and Services.
User	The username used during login.
Session start	The time at which the current session began, in 24-hour format.
Log out button	Users can log out of WorkPlace using this button, but this does not necessarily log them out of any applications that are running (depending on which user access agent is being used). To increase security, users should log out of or quit applications when they finish working with them, particularly when working on computers that are shared with other users.

Details	Users can click this button for system status information (not items appear for all users): • **Zone**: Security zones are used to allow or deny access to members of each community. • **Realm**: A realm allows users to authenticate using credentials stored on an external authentication server. • **Community**: Communities allow you to group realm members based on different security needs.

- For users accessing WorkPlace on small form factor devices, the WorkPlace appearance varies depending on the capabilities of the device. For more information, see End Point Control and the User Experience.
- On Windows systems, using browser toolbars with popup blocking enabled may prevent WorkPlace from closing any open Network Explorer and graphical terminal session windows when the main WorkPlace window is closed.
- Logging out of Outlook Web Access (OWA) during a WorkPlace session also logs the user out of WorkPlace. This is because the OWA logoff script clears all browser cookies, including the one used by WorkPlace. Users can simply close the browser window instead of logging out of OWA to work around this issue.

Intranet Address Field

If enabled, the **Intranet Address** field appears along the bottom of the WorkPlace page, except on small form factor devices, and gives users an alternate method to access Web resources, Windows network resources, and terminal servers.

When you set up communities within a realm (for example, a community of employees and one of partners), you can give each one a unique appearance, using WorkPlace styles and layouts. The WorkPlace layout determines whether the **Intranet Address** box is displayed for a particular community. See Creating or Editing a WorkPlace Layout for more information.

Configuring the functionality of the **Intranet Address** field is a global configuration setting. Depending on the configuration, users can type URLs to reach Web resources if WorkPlace is running in translated mode, or they can type UNC paths to reach file system resources. (If WorkPlace is running in non-translated mode, users can type URLs directly in the browser **Address** field.) This is especially useful if you have defined an entire DNS or Windows domain as a resource and want to give a group of users direct access to all the resources in that domain.

To access a Web resource or terminal server when WorkPlace is running in translated mode, the user types the URL in the **Intranet Address** field, and then clicks **Go**. If the user has appropriate access privileges, the resource then opens in a new browser window.

The **Intranet Address** field accepts a variety of user input for accessing Web resources and terminal servers. Here are some guidelines, as shown in the below table.

Intranet Address Input Guidelines

Element	Description
Resource address	A user can access a resource by typing a complete URL (domain and host name) or just a host name. For example, a user could access a resource named *CRM* on a host named fred using a full URL (such as `http://fred.example.com/CRM/`) or a host name (such as `http://fred/CRM/ or fred/CRM/`).
UNC path	To access a file system resource, the user types the UNC path (for example, `\\jax\software\download`) in the **Intranet Address** field, and then clicks **Go**. If the user has appropriate access privileges, the Network Explorer page displays, displaying the contents of the requested file system resource.
Protocol	The user does not need to include the `http://` protocol identifier to access a standard Web resource. To access a secure Web site, however, the user must include the `https://` protocol identifier. When specifying a terminal server resource name, users must include the appropriate protocol identifier in the URL. Supported terminal server types are Windows Terminal Services, which uses the `rdp://` identifier, and Citrix, which uses `citrix://`.
Port number	To access a Web resource on a non-standard port (that is, other than 80), the user must type the port number after the host name. For example, `fred:8080/SAP` and `https://fred:443/SAP` are both valid entries.

For information about configuring the **Intranet Address** field to allow access to UNC pathnames, URLs, or both, see Configuring WorkPlace General Settings.

Bookmarks

Users can create personal links in WorkPlace for quick access to any resources that they have privileges to use. This can include Workplace user-defined Web URL, RDP, VNC, Citrix, FTP, SSH, and Telnet bookmarks. Users can also minimize their bookmark list, edit the bookmark list, and edit individual RDP bookmarks.

WorkPlace personal links are similar to Web browser bookmarks or favorites lists except that they are stored on the SMA appliance, while standard browser bookmarks are stored on a specific computer. Users can access and manage their WorkPlace personal links whenever they are logged in to WorkPlace, regardless of the computer they are using.

When you set up communities within a realm (for example, a community of employees and one of partners), you can give each one a unique appearance, using WorkPlace styles and layouts. The WorkPlace layout determines whether the *Personal Bookmarks* group is displayed for a particular community. See Creating or Editing a WorkPlace Layout for more information.

ⓘ **NOTE:** To access non-HTTP resources (for example, an SMB host) through WorkPlace bookmarks, users must be running an access agent, such as one of the tunnel clients. For more information, see User Access Agents.

Custom RDP Bookmarks

Custom settings for user remote desktop links are managed through the Custom RDP Link window. Screen resolution and color depth can be controlled by either the user or administrator. Single sign-on allows the administrator to customize the user sign on to request specific credentials or enable specific domains.

Network Explorer Page

When a user accesses a file system resource (by clicking a network shortcut, typing a UNC path in the **Intranet Address** box, or clicking the **Network Explorer** link on the WorkPlace home page), the Network Explorer page is displayed.

Topics:

- The Network Explorer

The Network Explorer

The Network Explorer is the default interface on all devices. The Network Explorer enables users to work with network files and folders on a network using a Web browser much as if they were working locally on the network. The Network Explorer page displays shared folders or files that users have permission to access.

- Users can browse these domains, servers, shares, folders, and files by clicking links on the Network Explorer page.
- The navigation pane at the left displays a list of resources available to the user on your network.
- The pane on the right enables the user to work with folders and files.
- If the administrator has enabled upload functionality, and the user has write privileges, the user can upload files. See Configuring WorkPlace General Settings for more information.

For more detailed information about the Network Explorer, see the *Secure Mobile Access 12.4 Workplace User Guide*.

User Access Components and Services

Topics:

About User Access Components and Services

The SMA appliance includes several components that enable users to access resources on your network. This section describes each of the user access components and the services that control them.

Many of these components are provisioned or activated from the WorkPlace portal. For more information about WorkPlace, see The WorkPlace Portal.

User Access Agents

User access agents are deployed to client devices based on the community to which the user belongs. Most agents are deployed automatically when the user logs in to the WorkPlace portal using a browser. The installation package for these two access agents can also be made available for download from a file share on your network or deployed through applications such as Microsoft’s Systems Management Server (SMS) or IBM’s Tivoli. For more information, see Selecting Tunnel Access Methods for a Community.

When deployed automatically—when a user logs in using a browser—the access agents are both deployed and activated on the first visit. This generally requires the user to accept a download for the Secure Endpoint Manager (SEM), which will in turn manage the access agent installation and future access agent updates. On subsequent visits to the WorkPlace portal from the same client device using the same browser, the access agents are automatically activated without user intervention. See Client and Agent Provisioning (Windows) for more information.

The below table compares the capabilities of access agents and lists their requirements. For other system requirements, see Client Components.

ACCESS AGENT COMPARISON

	Network tunnel access (IP protocol)		**Proxy access (TCP protocol)**	**Web access (HTTP protocol)**
	OnDemand Tunnel agent	Connect Tunnel client	OnDemand Mapped Mode	Translated, Custom Port mapped, Custom FQDN mapped Web access
Application support				
TCP-based client/server applications	x	x	x	
TCP- or UDP-based client/server applications	x	x		
URLs and Web applications	x	x	x	x
Windows networking				
Web-based file access	x			x
Native Windows file access (Network Neighborhood)	x	x		
Mapped network drives	x	x		
Windows domain logon		x		
Connection types				
Forward connections	x	x	x	x
Reverse connections (such as FTP or SMS)	x	x		
Cross-connections (such as VoIP)	x	x		
Operating systems				
Windows	x	x	x	x
Linux		x		x
MacOS	x	x	x	x
Administrator privileges required to install client/agent	x	x		
Deployment				
Auto-activated from WorkPlace	x		x	x
Provisioned from WorkPlace	x	x	1	
Provisioned outside of WorkPlace		x		

1. Port-mapped mode requires ActiveX or Java. For a user without administrator rights who can’t run ActiveX, the Java Runtime Environment (JRE) is used.

Topics:

- Client and Agent Provisioning (Windows)
- WorkPlace
- Tunnel Clients
- Web Access

Client and Agent Provisioning (Windows)

Secure Endpoint Manager is a component that enables you to provision Windows users with EPC and access agents reliably when they log in to WorkPlace. It provides better application compatibility for applications that need an agent, and more reliable EPC interrogation; in addition, most client updates do not require administrator privileges. If something goes wrong during provisioning, the error is automatically recorded in a client installation log (identified by username) that you can view in AMC.

Installing Secure Endpoint Manager is a one-time step and does not require that the user have administrator privileges. The only other time users will be (briefly) aware of it once it’s installed is when an access agent or the Access Manager itself needs to be updated. Installing Secure Endpoint Manager is also not required, but users without it will have just Web-only access to resources in WorkPlace, or be forced to log out, depending on how you configure the community.

Topics:

- Secure Endpoint Manager
- Installing Secure Endpoint Manager
- Enabling Secure Endpoint Manager Software Update Policies
- Provisioning and Personal Firewalls
- Client Installation Logs

Secure Endpoint Manager

Secure Endpoint Manager (SEM) is a software component that is installed on a client device. It is installed when the SMA product is accessed from a Web browser. SEM enables a user on a client device to log in to an SMA appliance and perform tasks using a Web browser.

SEM provides the installation and activation of several client components, such as OnDemand Tunnel, End Point Control, OnDemand Mapped Mode, and Graphical Terminal Agents.

SMA provides an update policy for Secure Endpoint Manager (SEM) and its associated sub-components, such as Graphical Terminal Agents, End Point Control, OnDemand Tunnel, Web Proxy, and OnDemand Mapped Mode.

SEM installation and software update policies are supported on Windows and macOS client operating systems.

After the server-side firmware has been updated, SMA administrators can control and update specific user Groups and Communities individually, eliminating the need to update thousands of client devices simultaneously.

SEM software updates can be triggered using Web access or Tunnel access methods or using both methods.

Installing Secure Endpoint Manager

Users are normally required to install a Secure Mobile Access agent or client before they are granted access to network resources when they log in to WorkPlace. This is the recommended setting: it provides better compatibility for applications that need an agent, which means broader access for users and fewer Help Desk calls for you. Users logging in to WorkPlace are offered these choices when this setting is enabled:

- **Install**: Secure Endpoint Manager is installed on the user's computer. Users will need to do this only once.
- **Logout**: The user's session is ended.

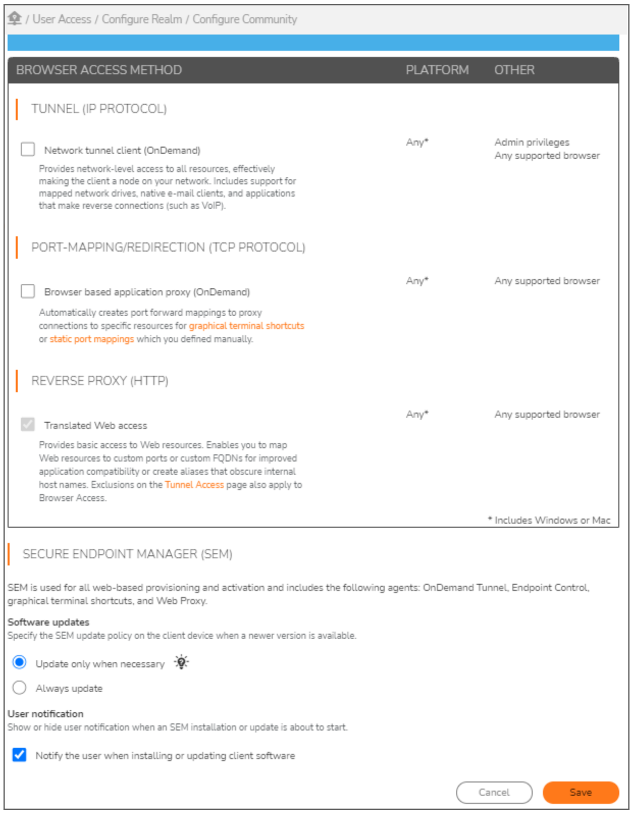
If you configure the community such that an agent or client is not required, users are offered these choices when they log in:

Install: Secure Endpoint Manager is installed on the user's computer. Users will need to do this only once.

△ **CAUTION: In this scenario (assuming EPC is enabled), the user is placed in either the Default zone or a Quarantine zone, depending on how the community is configured. A Quarantine zone may be too restrictive, and the Default zone probably needs to accommodate many other types of users. You might want to create a unique, Web-only zone for users who don't require an agent. See Scenario 3: Employees Connecting from a Public Kiosk for ideas on how to set up this kind of zone.**

Enabling Secure Endpoint Manager Software Update Policies

Software update policies for Secure Endpoint Manager (SEM) are enabled at the Community level.



/ User Access / Configure Realm / Configure Community

BROWSER ACCESS METHOD	PLATFORM	OTHER
TUNNEL (IP PROTOCOL)		
□ Network tunnel client (OnDemand) Provides network-level access to all resources, effectively making the client a node on your network. Includes support for mapped network drives, native e-mail clients, and applications that make reverse connections (such as VoIP).	Any*	Admin privileges Any supported browser
PORT-MAPPING/REDIRECTION (TCP PROTOCOL)		
□ Browser based application proxy (OnDemand) Automatically creates port forward mappings to proxy connections to specific resources for graphical terminal shortcuts or static port mappings which you defined manually.	Any*	Any supported browser
REVERSE PROXY (HTTP)		
☑ Translated Web access Provides basic access to Web resources. Enables you to map Web resources to custom ports or custom FQDNs for improved application compatibility or create aliases that obscure internal host names. Exclusions on the Tunnel Access page also apply to Browser Access.	Any*	Any supported browser

* Includes Windows or Mac

SECURE ENDPOINT MANAGER (SEM)

SEM is used for all web-based provisioning and activation and includes the following agents: OnDemand Tunnel, Endpoint Control, graphical terminal shortcuts, and Web Proxy.

Software updates

Specify the SEM update policy on the client device when a newer version is available.

● Update only when necessary

○ Always update

User notification

Show or hide user notification when an SEM installation or update is about to start.

☑ Notify the user when installing or updating client software

To enable an automatic software update policy for Secure Endpoint Manager:

1. Log in to AMC.
2. Navigate to **User Access** > **Realms** > ***{Your Realm}*** > **Communities** > ***{Your Community}*** > **Browser Access** page.

   The Secure Endpoint Manager (SEM) panel is near the bottom of the page.

   There are three options that can be configured for the SEM Software Update Policy:

   - **Update only when necessary** – Select this option if you want the SEM to be updated on client devices based on the following criteria whether or not it is necessary. The following criteria triggers an update:
     - When Personal Device Authorization is not enabled on any client version 11.4 and older. Clients running versions 12.X.X are not prompted for updates.
     - When Personal Device Authorization is enabled on any client version 11.4 and older.

     When the **Update only when necessary** option is selected, updates and installations are performed whenever an update is **required** by the **system** or whenever an update is required by the administrator.
   - **Always update** - Select this option if you want the SEM to always be kept up-to-date on client devices. This includes differences in hotfix, maintenance, and major releases (any differences in those triggers an update).

When the **Always Update** option is selected, when a user logs in, they are given a choice to update the SEM or log out.

- **User notification** - Select the **Notify the user when installing or updating client software** option if you want notifications to be sent to the user about the SEM during an installation or an update. This is controlled by the AMC administrator and applies to both installations and updates of the SEM.

  In cases where SEM is required, either Access Agents or EPC must be provisioned. Otherwise, the SEM installation or update cannot run.

Provisioning and Personal Firewalls

Some third-party firewall products regulate outbound connections by process (in addition to port and protocol). These firewalls may raise a security alert regarding Secure Endpoint Manager during the provisioning of agents or EPC components. In most cases, the user should be instructed to “unblock” or “permit” the outbound connection.

There are a few firewalls, such as one supplied by Trend Micro, that do not permit a user with restricted rights to override firewall settings. For corporate systems on which users have limited access rights, you may want to update the firewall settings before deploying the Secure Mobile Access VPN so that users won’t have to respond to these security prompts. See Using Personal Firewalls with Agents for more information.

Client Installation Logs

If something goes wrong during client or agent installation on a computer running Windows, the error is recorded in a client installation log on the user’s local computer. These logs are automatically uploaded to the appliance and listed in AMC if the user has Secure Endpoint Manager installed. For more information, see Client Installation Logs (Windows).

WorkPlace

WorkPlace is a Web-based portal that provides dynamically personalized access to Web resources protected by the Web proxy service. After a user logs in to WorkPlace, a home page displays that contains an administrator-defined list of shortcuts. These shortcuts point to Web-based file shares, Web-based applications, and terminal server resources to which the user has access privileges.

All Secure Mobile Access user access components are provisioned or activated through the WorkPlace portal. WorkPlace is accessible from any standard Web browser. For more information, see The WorkPlace Portal.

WorkPlace Sites

You can create multiple WorkPlace sites for different user segments, such as employees, business partners, and suppliers. Each site can have a unique external URL and a unique appearance, or bypass the WorkPlace portal and redirect the user to a different start page.

For example, you could create a WorkPlace site for your employees with a customized title and logo, and a URL of *`http://employees.headquarters.com`*, and create a different site for your partners at `http://partners.subsidiary.com`. If you create multiple WorkPlace sites with unique external URLs, you can import a wildcard certificate to the appliance and designate it as the server certificate for multiple WorkPlace sites, or procure a separate SSL certificate for each site whose FQDN is different from the appliance's domain name. For more information, see Certificates.

ⓘ **NOTE:** Due to client operating system limitations, Mobile Connect cannot convert host name, URL, or domain type resources containing wildcards to an IP address and, therefore, cannot redirect them to the appliance.

Optionally, if you have configured multiple realms, you can associate a WorkPlace site with a realm; this enables users to bypass the portion of the authentication process in which they would normally specify a realm to log in to. If you associate a WorkPlace site with a realm, users cannot select a different realm to log in to; a user who does not belong to the specified realm cannot log in to the specified WorkPlace site.

You can customize the following components of WorkPlace:

- Company logo
- WorkPlace title
- Greeting at top of page
- Color scheme
- Help file
- Font family

You can have users bypass the WorkPlace portal and go directly to a different start page, provided that the realm they log in to allows translated, custom port mapped, or custom FQDN mapped Web access exclusively. See Adding WorkPlace Sites for more information.

You may also want to set up custom licensing agreements that they will have to accept before getting started.

The URL a user types to log in to WorkPlace is preceded by the `http://`protocol identifier. The Web session is then redirected to a site that uses secure HTTP (HTTPS) and uses the `https://`protocol identifier.

ⓘ **NOTE:**

- If you do not specify a custom WorkPlace site, or if users access the appliance using its default name, the default WorkPlace site is automatically used.
- Rather than creating a new WorkPlace site from scratch, you can save time by making a copy of an existing site and changing some parameters to fit the new site. For information about copying a WorkPlace site, see Adding, Editing, Copying, and Deleting Objects in AMC.
- You can delete a WorkPlace site if you no longer need it, but you cannot delete the default WorkPlace site. For information about deleting WorkPlace sites, see Adding, Editing, Copying, and Deleting Objects in AMC.

Topics:

Adding WorkPlace Sites

AMC includes a preconfigured default WorkPlace site. You can create additional WorkPlace sites as needed; this section describes how to do so.

You can make WorkPlace look different, on a per-community basis, if you set up different styles and layouts. For more information, see Modifying the Appearance of WorkPlace. For information about configuring WorkPlace sites for small form factor devices, see WorkPlace and Small Form Factor Devices.

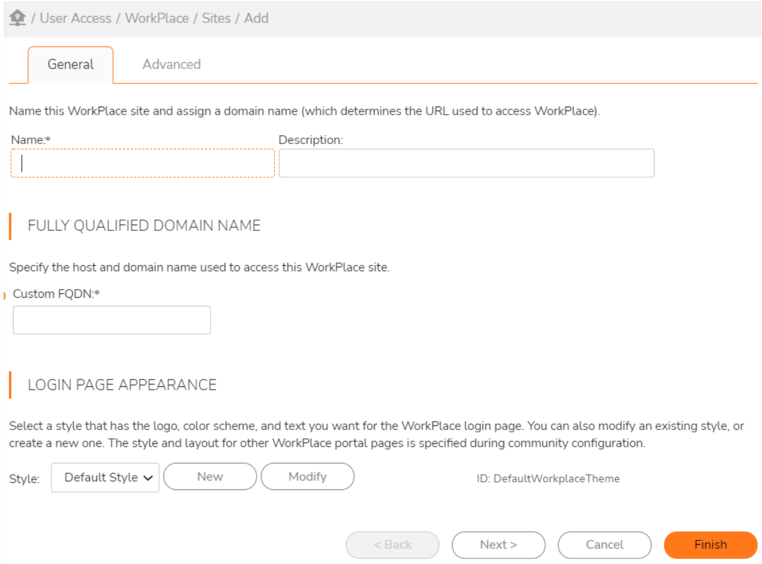
The fully qualified domain name (FQDN) for the WorkPlace site can include one of the following:

- A host within the same domain name as the SMA appliance.
- A custom FQDN. This option can use a wildcard SSL certificate when its IP address is the same as another WorkPlace site that uses the wildcard certificate, or you can use a separate SSL certificate for the site. Before creating the site, you must obtain the certificate. For more information, see Certificates.

In either case, you must communicate the external FQDN to users so they know how to access WorkPlace. You must also add this FQDN to your public DNS.

To add a WorkPlace site:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **WorkPlace Sites** tab.
3. Click the **+** (New) icon.
   The **Configure WorkPlace Site** page displays.



/ User Access / WorkPlace / Sites / Add

Name this WorkPlace site and assign a domain name (which determines the URL used to access WorkPlace).

Name:*

Description:

FULLY QUALIFIED DOMAIN NAME

Specify the host and domain name used to access this WorkPlace site.

Custom FQDN:*

LOGIN PAGE APPEARANCE

Select a style that has the logo, color scheme, and text you want for the WorkPlace login page. You can also modify an existing style, or create a new one. The style and layout for other WorkPlace portal pages is specified during community configuration.

Style: Default Style

ID: DefaultWorkplaceTheme

4. In the **Name** field, type a unique name for the WorkPlace site.
5. (Optional) In the **Description** field, type a descriptive comment about the WorkPlace site.
6. Type the IPv4 or IPv6. By default, AMC listens on all interfaces for all services and connects the request to the correct service based on the FQDN being requested.

7. **(Migrated/imported configurations only)** An additional listening address can be specified if AMC was upgraded from a previous version where a virtual IP address is configured for the WorkPlace site or the CEM is used.

   For migrated/imported configurations with existing virtual hosts, the UI section is visible, but the Administrator cannot create new virtual addresses. If necessary, use CEM to create virtual host addresses in a new or migrated/imported configuration.

   If the host name or IP address on the certificate does not match the **Custom FQDN** or **IP address** that you specified for this site, a security warning is displayed when users access the site.

8. Select a style—which includes the logo, color scheme, and text—for the WorkPlace login page. The style and layout for other WorkPlace portal pages is specified during community configuration; see Modifying the Appearance of WorkPlace for information on modifying or creating a style.

9. Click **Next** to open the **Advanced** page.

10. In the **Realm** area, select one of these options:

    - **Log in using this realm**: Users are not prompted to select a realm, and only members of the specified realm can access the WorkPlace site.
    - **Prompt user for realm**: Offer users a list of realms from which to choose. You can offer them all configured realms, or clear the **All realms** selection and choose the ones that should be in the list. Any authorized user can access the WorkPlace site after selecting a realm during login.

11. In the **Start page** area, select **Display this page after authentication** if you want users to bypass the default WorkPlace home page after authentication. For example, if you have someone who will submit content using a Web-based content management system, this setting allows you to present the writer with the CMS interface immediately after he or she logs in.

    This setting is available only if the realm specified in the **Realm** area offers translated, custom port mapped, or custom FQDN mapped Web access exclusively. The URL you enter in this text box will be automatically prefixed with `http://`. If this is a URL for a secure site, you must include the `https://` protocol identifier.

    If you specify an alternate page for users and they bypass the default WorkPlace portal, the user's session is valid as long as the browser window is open, or until the session times out. Unlike the WorkPlace portal, the alternate page will not include a **Log out** option.

12. Click **Finish** to save your WorkPlace site settings.

ⓘ **NOTE:** You can enter a URL alias in the **Start page** area (if you don’t want users to see the complete URL in WorkPlace), provided that you create a URL resource for it. For example, if you define a URL resource as *`http://intranet.mycompany.com`* with an alias of intranet, you can specify the start page for WorkPlace here simply with intranet (or a more specific path, such as intranet/some/path). When users authenticate, they are redirected to `https://<appliance>/intranet` or `https://<appliance>/intranet/some/path`.

Modifying the Appearance of WorkPlace

When you create a new WorkPlace site, you have control over the look-and-feel of the pages and the organization of resource shortcuts and other elements, such as intranet browsing and Network Explorer. The appearance of WorkPlace is controlled by the following design elements, which can be created and reused:

- A *WorkPlace style* determines the color scheme, fonts, and images used in WorkPlace. A style can be applied to two groups of pages: those that contain user resources, and the login, error, and notification pages.

  An important thing to remember is that WorkPlace login, error, and notification pages are assigned a style when you configure a *WorkPlace site* (see Adding WorkPlace Sites for more information), and the portal pages are assigned a style when you configure a *community* (see Creating and Configuring Communities for more information).

- A *WorkPlace layout* determines elements like WorkPlace navigation, the number of columns on a page, whether users see the **Intranet Address** box, and which shortcuts appear and how they are arranged. A layout applies only to WorkPlace resource pages.

  If your site requires a complete overhaul of the way WorkPlace looks and you are familiar with creating Web content and style sheets (`.css`), you can upload a complete style to the appliance and then select it when you create your site and assign it a style. See Fully Customizing WorkPlace Pages for more information. To do further customization—for example, to insert a use agreement into the login process—see About Custom WorkPlace Templates.

ⓘ | **NOTE:** The Default Style and Default Layout for WorkPlace cannot be deleted.

Topics:

- Creating or Editing a WorkPlace Style
- Creating or Editing a WorkPlace Layout

About Custom WorkPlace Templates

There are situations in which you need to completely customize the way that WorkPlace looks and what steps are involved in the login process. For example:

- You may want to use your existing corporate portal (where that portal application has been defined as a resource) instead of WorkPlace. Here you would customize the login, logoff, notification, and error pages to match the look and feel of your existing portal.
- You might want to provide access to a specific application (which has been defined as a resource) to a business partner. Here you would customize the login, logoff, notification, and error pages to match the look and feel of the application.

The templates you can customize fall into three categories, see the below table. If you modify the ones in one category, you should probably also modify the others to ensure consistency.

Custom WorkPlace Template Types

Template type	Description
Authentication	The pages used to gather a user’s credentials, including selecting a realm and entering a username, password, or passcode. You might use these templates to provide the user with on-screen information about how to log in to your network.

Error	The pages displayed when an error occurs, such as invalid user input (an authorization-denied message or a failed login), or an error in the appliance. You might use these templates to provide the user with support information, such as administrator contact information and where to find user guides.
Notification	The pages that provide the user with basic information required to interact with the system, including the logout page (confirming successful logout) and pages containing messages from the authentication module (such as a password-expiration warning).

Although you can redesign the layout or add graphics and text on these pages, you cannot modify or remove the existing elements. For example, on the authentication page you cannot rename the **Login** button. These elements are dynamically generated by WorkPlace.

The WorkPlace pages that are presented to the user after login cannot be customized manually; they are controlled from AMC.

How Template Files are Matched

You can customize templates globally, or on a per-WorkPlace site basis. For example, you might customize the global templates to use one design, and then override that design on a site-by-site basis by modifying its templates.

When a user connects to a WorkPlace site, the appliance first looks for the most specific template. If one is not found, it checks for the generic template for the category (authentication, error, or notification). If neither is found, the default WorkPlace template (the one under AMC's control) is used.

The following tables list the templates available for full-screen devices (desktops and laptops), along with the corresponding file names. For small form factor devices, prefix the file names as follows:

- For smartphone and PDA devices, prefix the file name with `compact-`.
- For WAP devices, prefix the file name with `micro-`.

For example, to customize the page users see when selecting a realm, edit `realm-select.tmpl`. The equivalent pages for smaller devices are `compact-realm-select.tmpl` (for smart phones and PDAs), and `micro-realm-select.tmpl` (for WAP devices).

Customizing WorkPlace Templates

The appearance of WorkPlace is controlled using several templates. To customize the templates, you create an HTML file (or, in the case of a small form factor device, an `xHTML` or `cHTML` file) using any standard Web design tool or text editor.

If your customization includes graphics, upload them to this folder:

```
/usr/local/extranet/htdocs/__extraweb__/images
```

If an `images` directory is not already present, you can create it by typing the following command:

```
mkdir -p /usr/local/extranet/htdocs/__extraweb__/images
```

The file names you must use are described in How Template Files are Matched. For small form factor devices, a prefix is added:

- For smartphone and PDA devices, prefix the file name with `compact-`.
- For WAP devices, prefix the file name with `micro-`.

To customize the WorkPlace templates for desktop devices:

1. Create an HTML file containing the desired layout, and add the WorkPlace-specific tags:
   - Within the `BODY` tag, add an `HTML COMMENT` tag containing the word `EXTRAWEB`:

     ```
     <!-- EXTRAWEB -->
     ```

     This tag is required; it determines where to place content dynamically generated by the appliance. Without it, the user trying to log in to WorkPlace will be repeatedly sent back to the beginning of the authentication process.
   - Add a reference to the external JavaScript file:

     ```
     <script language="javascript"
     src="/__extraweb__/template.js"></script>
     ```

   - To have your templates display any WorkPlace content (including the `.css` file or the custom logo you configured in AMC), modify your HTML code to reference the `/__extraweb__/images/` path. For example:

     ```
     <img src="/__extraweb__/images/mylogo.gif">
     ```

2. Save the file with the appropriate file name using a `.tmpl` file extension.

To customize the WorkPlace templates for small form factor devices:

1. Create a file in xHTML (for smart phones or PDAs) or cHTML (for WAP devices) format containing the desired layout, and add the WorkPlace-specific tags:
   - Within the `BODY` tag, add a `COMMENT` tag containing the word `EXTRAWEB`:

     ```
     <!-- EXTRAWEB -->
     ```

     This tag is required: it determines where to place content dynamically generated by the appliance. Without it, the user trying to log in to WorkPlace will be repeatedly sent back to the beginning of the authentication process.
   - To have your templates display any WorkPlace content (including the `.css` file or the custom logo you configured in AMC), modify your code to reference the `/__extraweb__/images/` path. For example:

     ```
     <img src="/__extraweb__/images/mylogo.gif">
     ```

2. Save the file with the appropriate file name using a `.tmpl` file extension.

Working with WorkPlace Shortcuts

WorkPlace enables users with appropriate access privileges to use a Web browser to access Web resources, terminal servers, and files and folders on a Windows file server. Even though you may have defined your resources in AMC, none of them appear in WorkPlace until you create corresponding shortcuts. This section explains how to create and manage the shortcuts and shortcut groups in WorkPlace.

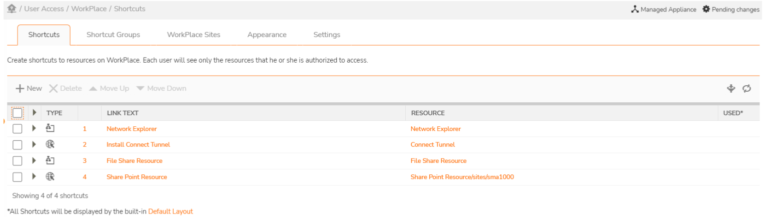
For information about enabling access to file system resources, file uploads, and the **Intranet Address** field, see Configuring WorkPlace General Settings.

Adding Web Shortcuts

Web shortcuts give your users quick access to Web resources. Before you can create a shortcut to a Web resource, you must first define the resource; for more information, see Adding Resources.

To add a Web shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts** tab.

   / User Access / WorkPlace / Shortcuts

   Managed Appliance Pending changes

   Create shortcuts to resources on WorkPlace. Each user will see only the resources that he or she is authorized to access.

□	TYPE		LINK TEXT	RESOURCE	USED*
□		1	Network Explorer	Network Explorer	
□		2	Install Connect Tunnel	Connect Tunnel	
□		3	File Share Resource	File Share Resource	
□		4	Share Point Resource	Share Point Resource/sites/sma1000	

   Showing 4 of 4 shortcuts

   *All Shortcuts will be displayed by the built-in Default Layout

3. Click the **+** (New) icon.
4. Select **Web shortcut** from the dropdown list.

   The **Add Web Shortcut** page displays.
5. In the **Position** field, select the number that specifies the position of the shortcut in the list.
6. In the **Resource** drop-down menu, select the resource to which this shortcut will be linked. This list contains the available URL resources that are defined on the **Resources** page in AMC. For example, when adding a shortcut to SharePoint, you could define a URL resource specifying the resource Name as *SharePoint* and the resource URL as `http://intranet.sharepoint.com`. Then, you would select *SharePoint* in the **Resource** drop-down menu.

   For more information about defining resources, see Creating and Managing Resources.
7. Specify the link and descriptive text that users will see in WorkPlace. The entries can include variables to make them even more user- or session-specific; see Using Variables in Resource and WorkPlace Shortcut Definitions for more information.

   - In the **Link text** field, type the hyperlink text that users will click to access the Web resource. The **Link text** should be no longer than 25 characters.
   - In the **Description** field, type a descriptive comment about the shortcut. Although optional, a description helps users identify the Web resource. The comment appears next to the link.
8. Use the **Shortcut group** area to either add this shortcut to an existing group, or put it in a new one. Groups are one of the organizational elements in a WorkPlace layout. You could, for example, put all client downloads for users in a group, and then (on the **Configure WorkPlace Layout** page) put the group in a column or on its own WorkPlace page.
9. To specify additional options, click **Next**.

   The **Advanced** tab of the **Add Web Shortcut** page displays.

10. Under **Make link available to these devices**, associate the WorkPlace shortcut with the device types that can be used to access it:

    - If you select **All devices**, the shortcut will appear on all devices types, regardless of whether the Web resource itself is supported on all device types.
    - To restrict display of the shortcut to only certain types of devices, clear the **All devices** checkbox, and then select just the device types that are supported.

    For example, WorkPlace supports a variety of small form factor devices, but not all Web resources are compatible with all devices. Outlook Web Access is available only on standard browsers, while Outlook Mobile is available only on small form factor devices. So if you have Outlook Mobile set up as a resource, you should select both the basic and advanced mobile devices.

11. Use the **Start page** field, if necessary, to append more specific information to the selected URL. For example, if you want the link to point to a directory or file other than the root, type a relative path in the **Start page** field.

    This is useful for Web applications that store their content in a location other than the root. For example, if the selected URL is for Outlook Web Access and it points to *`mail.example.com`*, you could set the start page to *`/exchange/root.asp`*.

    The resulting URL would be *`https://mail.example.com/exchange/root.asp`*.

    For SharePoint, set the start page to the extended path, such as *`Pages/Default.aspx`* or *`SitePages/Home.aspx`*. For SharePoint shortcuts, the basic hostname/<IP address> of the SharePoint server is defined on the **Resources** page in AMC. The extended path is configured here as the **Start Page**.

Viewing Shortcuts

As the administrator, you see the entire list of shortcuts you have configured in AMC; however, when a user logs into WorkPlace, the list is filtered to display only the resources that he or she has permission to use, based on your policy and the type of device for which the shortcut is enabled. All types of shortcuts (Web, network, and graphical terminal) and groups of shortcuts are displayed in AMC and WorkPlace. How they are laid out is determined by the WorkPlace layout in use for a given community.

To view shortcuts in AMC:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Optionally use the **Filters** settings to display only the objects you are interested in.

   For information about using filters, see Filters.
3. Review the data in the **Shortcuts** list:
4. Use the checkboxes to select the shortcuts you want to move or delete.

   - To display configuration details about a shortcut, click the plus sign (**+**) next to it. You'll see the description, what shortcut group it belongs to, if any, whether it is restricted by device type, and the names of any WorkPlace layouts to which it belongs.
   - The number indicates the order in which the shortcut is listed in WorkPlace. You can change this order here, or edit the list of shortcuts associated with a layout on the **Configure WorkPlace Layout** page. For more information, see Creating or Editing a WorkPlace Layout.

- The **Type** column indicates the type of shortcut.

  The supported shortcut types are Web, network, and graphical terminal.
- The **Link Text** column displays the hyperlink text that users see.
- The **Resource** column displays the name of the resource as defined on the **Resources** page in AMC.

  For more information about configuring resources, see Creating and Managing Resources.
- The **Used** column indicates whether the shortcut is included in a group or WorkPlace layout.

Editing Shortcuts

You can create new WorkPlace shortcuts when defining resources, but to edit or delete them, you must use the **Shortcuts** page.

To edit a shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the number or the link text of the shortcut that you want to edit.
3. Make edits as needed, and then click **Save**.

If you delete a shortcut, users will no longer see it in WorkPlace. To delete a shortcut, you must use the **Shortcuts** page.

To delete a shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Select the checkbox to the left of any shortcuts that you want to delete, and then click **Delete**. Deleting a shortcut does not delete the resource to which it refers.

WorkPlace displays the list of shortcuts in the same order as they appear on the **Shortcuts** page. You can move one or more shortcuts at the same time. The order of shortcuts (and groups of shortcuts) can be changed later in the layout you choose for your WorkPlace site, on the **Configure WorkPlace Layout** page.

To move one or more shortcuts:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Select the checkbox to the left of any shortcuts that you want to move.
3. Click **Move Up** or **Move Down** as appropriate.

   Each click of the button moves the selected shortcuts up or down one row.

To reorder an individual WorkPlace shortcut, an alternative method is to click its number or link text and then type its new list position in the **Position** field.

Creating a Group of Shortcuts

You can group Web and network shortcuts together for better WorkPlace organization and a more streamlined look. The WorkPlace user has the option of collapsing a group of file shares.

Users see only the groups to which they are permitted access. To create a group, you select from among existing WorkPlace shortcuts (not resources). Shortcuts can be members of more than one group.

To create a group of shortcuts:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts Groups** tab.
3. Click the **+** (New) icon.
4. The **Name** field, enter a name.
5. (Optionally), in the **Description** field, enter a description for the group.

   The description appears below the group's name in WorkPlace.
6. In the **Position** field, select the number that specifies the position of the shortcut in the list. The order of shortcuts and groups can be changed later in the layout you choose for this WorkPlace site, on the **Configure WorkPlace Layout** page.
7. Existing shortcuts are listed: select the ones that you want to add to this group and click **Save**. An individual shortcut can be a member of more than one group. You can also opt to save an empty group (without any shortcuts selected), and then edit it later.

Adding Network Shortcuts

Network shortcuts provide your users with quick access to file system resources. Before you can create a shortcut to a file system resource, you must first define the resource (see Adding Resources for more information).

To add a network shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts** tab.
3. Click the **+** (New) icon.
4. Select **Network shortcut** from the dropdown menu.

   The **Add Network Shortcut** page displays.
5. In the **Position** field, select the number that specifies the shortcut's position in the list.
6. In the **Resource** drop-down menu, select the file system resource to which this shortcut should be linked. This menu contains the file system resources that are defined on the **Resources** page in AMC; *Network Explorer*, for example, is a built-in resource for which you can configure a shortcut here. For more information about defining resources, see Creating and Managing Resources.
7. Specify the link and descriptive text that users will see in WorkPlace. The entries can include variables to make them even more user- or session-specific:
   - In the **Link text** field, type the hyperlink text that users will click to access the file system resource. The **Link text** should be no longer than 25 characters.
   - In the **Description** field, type a descriptive comment about the shortcut. Although optional, a

description helps users identify the file system resource. This comment appears beside the link in WorkPlace.

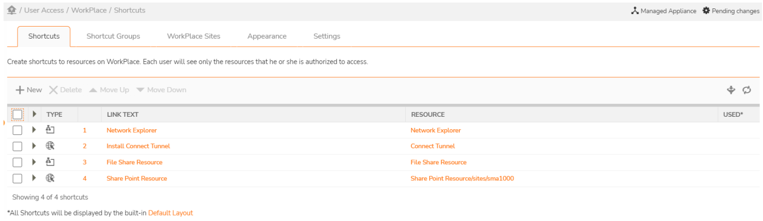
8. Groups are one of the organizational elements in a WorkPlace layout. Use the **Shortcut group** area to either add this shortcut to an existing group, or put it in a new one. You could, for example, put all file system-related shortcuts in a group, and then (on the **Configure WorkPlace Layout** page) put the group in a column or on its own WorkPlace page.

Adding a Virtual Desktop Shortcut

Use this page to create or edit the virtual desktop shortcuts appearing in WorkPlace. These shortcuts enable users to easily connect to VMware View resources.

To add a virtual desktop shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts** tab.



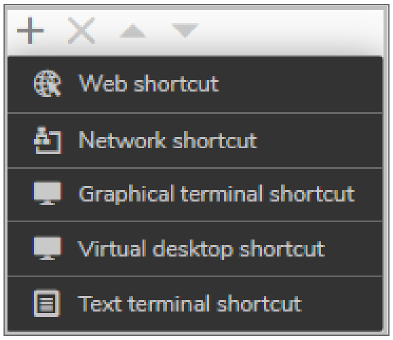
Create shortcuts to resources on WorkPlace. Each user will see only the resources that he or she is authorized to access.

TYPE		LINK TEXT	RESOURCE	USED*
	1	Network Explorer	Network Explorer	
	2	Install Connect Tunnel	Connect Tunnel	
	3	File Share Resource	File Share Resource	
	4	Share Point Resource	Share Point Resource/sites/sma1000	

Showing 4 of 4 shortcuts

*All Shortcuts will be displayed by the built-in Default Layout

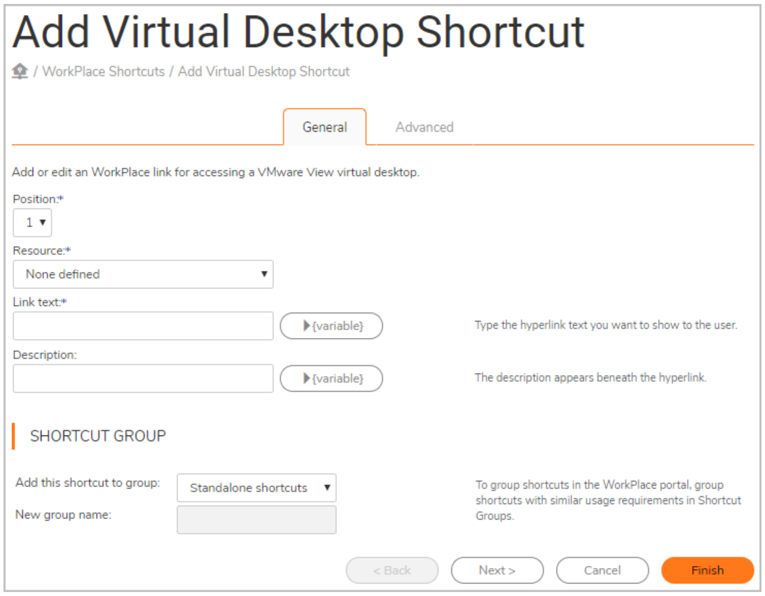
3. Click the **+** (New) icon.



4. Select **Virtual desktop shortcut** from the dropdown list.

   The **Add Virtual Desktop Shortcut** page displays.

5. On the **General** tab, select the resource from the **Resources** list.



Add Virtual Desktop Shortcut

/ WorkPlace Shortcuts / Add Virtual Desktop Shortcut

Add or edit an WorkPlace link for accessing a VMware View virtual desktop.

Position:* 1

Resource:* None defined

Link text:* Type the hyperlink text you want to show to the user.

Description: The description appears beneath the hyperlink.

SHORTCUT GROUP

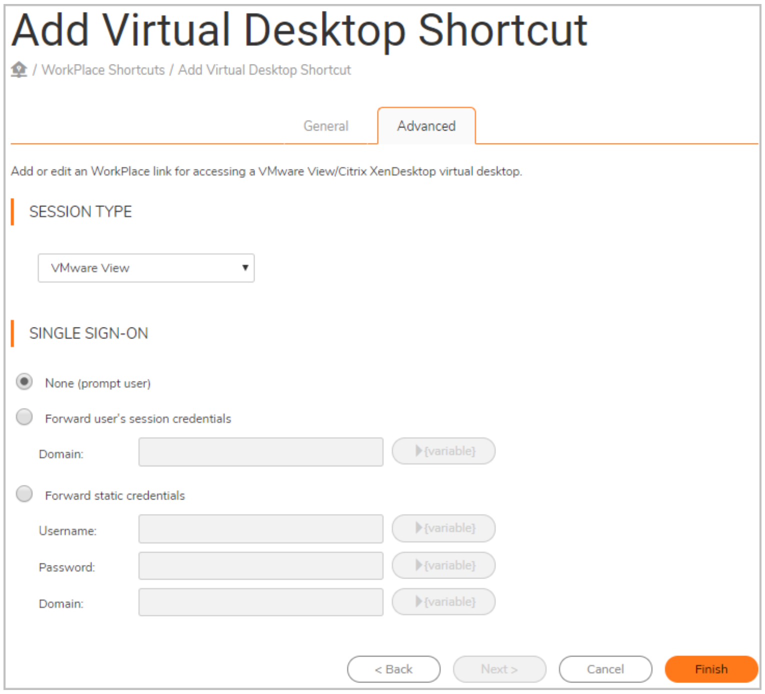
Add this shortcut to group: Standalone shortcuts

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

6. In the **Link Text** field, type in the hyperlink text that will appear as the shortcut for a VMware View host.
7. Type a description for the shortcut into the **Description** field.
8. In the **Add this shortcut to group** drop-down menu, select **Standalone shortcuts** if you do not want to make this shortcut part of a group, or select an existing group from the list. To create a new group, select **New**.
9. If you selected **New**, type a name for the new group in the **New group name** field.
10. Click **Next**.

    The **Advanced** tab displays.



Add Virtual Desktop Shortcut

/ WorkPlace Shortcuts / Add Virtual Desktop Shortcut

Add or edit an WorkPlace link for accessing a VMware View/Citrix XenDesktop virtual desktop.

SESSION TYPE

VMware View ▾

SINGLE SIGN-ON

● None (prompt user)

○ Forward user's session credentials

Domain: [ ] {variable}

○ Forward static credentials

Username: [ ] {variable}

Password: [ ] {variable}

Domain: [ ] {variable}

11. Select the session type, such as **Citrix XenDesktop** or **VMware View**.
12. In the **Single sign-on** area, specify how you want user credentials to forwarded to the host:
    - Click **None** to disable single sign-on and prompt the user for credentials.
    - Click **Forward user's session credentials** to pass the username and password used to authenticate to WorkPlace along to the host.
    - Click **Forward static credentials** to forward the same username and password for all users. Type the static **Username**, **Password**, and **Domain** to be forwarded for all users.
    - Click the associated **{variable}** button to expose the variable list and insert a variable into the above fields.
13. In the **Resource redirection** area, specify how you want the Virtual Desktop to interface with the to the host:
    a. To play audio generated by the remote device on the local computer, check the **Bring remote audio to local computer** checkbox.
    b. To copy the clipboard contents between computers, check the **Share clipboard between local and remote computers** checkbox.
    c. To access drives and/or printers on the remote device, check the **Drives** and/or **Printers** checkbox.
14. In the **Display properties** area, specify how you want the Virtual Desktop display to look:
    a. Use the **Screen resolution** drop-down menu to select the screen resolution for the Virtual Desktop display.
    b. Use the **Color depth** drop-down menu to select the color depth for the Virtual Desktop display.

15. Click **Finish**.

Web Shortcut Access

The SMA appliance offers two options for providing access to basic Web (HTTP) resources through WorkPlace shortcuts for users who are running the OnDemand Tunnel agent:

- **Redirect through network agent**: When this method is enabled, Web content is proxied through the appliance for users running the OnDemand Tunnel agent, provided that the agent is loaded. In this method, Web traffic from Workplace links does not use translation, does not support single sign-on, and does not use URL-based rules to control access. However, this method generally provides better application compatibility than the **Web content translation** option does.

  If you enable this setting, you can optionally configure selected WorkPlace resources to be translated by defining aliases for those specified resources. You can also enforce policy at the URL level and support single sign-on using this approach. For more information, see Adding Web Application Profiles.

- **Web content translation**: Web content is translated using the Secure Mobile Access Web translation engine, a reverse proxy that provides single sign-on and fine-grained access control. When this method is enabled, you can provide single sign-on and use URL-based rules to control access; however, this method provides more limited application compatibility than the **Redirect through network agent** option does. To provide single sign-on, you must specify an alias to the resource; for more information, see Adding Resources.

The Web shortcut access method you choose will depend on several factors, including the network protocols used by your applications, your security requirements, convenience for end users, and the target platforms. This option is configured on the WorkPlace **Settings** page.

Configuring WorkPlace General Settings

This section describes how to configure the WorkPlace general settings that apply to any WorkPlace site that you create. You decide here whether to enable access to UNC pathnames, URLs, or both in the **Intranet Address** box, but your WorkPlace layout determines whether the **Intranet Address** box is displayed for a particular community.

You can customize WorkPlace to varying degrees:

- You can modify the appearance of WorkPlace by setting up a style that uses a particular logo, color scheme, and greeting text. For a consistent look, this same style can be specified for the site's login, error, and notification pages. See WorkPlace Sites for more information.
- For sites that require even more control over the look and feel of WorkPlace, see Fully Customizing WorkPlace Pages.

To configure WorkPlace general settings:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **WorkPlace**, click **Configure**.

   The **Settings** tab for **WorkPlace** appears.

3. Select one of the **Web Shortcut Access** options. This setting determines how URL resources are accessed if WorkPlace activates the tunnel agent. For information about these options, see Web Shortcut Access.

   - **Redirect through network agent**: Web content is proxied through the appliance for users running the OnDemand Tunnel agent.
   - **Use Web content translation**: Web content is translated using the Secure Mobile Access Web translation engine.

4. If the layout specified for your WorkPlace site includes the **Network Explorer** resource, users will have access to file system resources from the Network Explorer page in WorkPlace. Select **Enable file uploads to < > megabytes** to enable users to upload files to a Windows file system resource. This setting takes precedence over any permissions you set in a file system access control rule. If an access rule grants a user write access to a file system but file uploads are disabled for the WorkPlace service, the user can only move and delete files, not write to them.

   A single file upload cannot exceed the number of megabytes you specify. Enabling users to upload large files may have a negative effect on the performance of the appliance.

5. In the **Intranet Address Box** area, specify settings that control the functionality of the **Intranet Address** box in WorkPlace. (Whether the **Intranet Address** field is available is specified in your WorkPlace layout and also depends on your device: it cannot be displayed on mobile devices.)

Select **Enable access to UNC pathnames and Enable access to URLs** if you want to enable users to reach a Web resource by typing its UNC pathname or URL in the **Intranet Address** field on WorkPlace. This can be useful if, for example, you have defined an entire DNS domain as a resource and want to provide access to all Web servers within the domain without needing to define each individual Web resource in the domain. This setting applies only when WorkPlace is running in translated mode.

For information about defining Web resources, see Adding Resources.

ⓘ | **NOTE:**

- The settings that you specify in the **Intranet Address** field have no effect on your access control policy. For a detailed discussion of this feature, see Intranet Address Field.
- If you are concerned that user credentials may be stolen, you can offer (or require) that users logging in to WorkPlace provide their credentials by pointing to characters on a keyboard display instead of typing them. See Using the Virtual Keyboard to Enter Credentials for more information.

Topics:

Web Only Access

The Web Only Access feature for SMA supports HTML and enables users to access HTML Web sites. Web Only Access for SMA also enables users to access on-demand computing services using only a web browser. Users can use Connect Tunnel (CT) and Native Access Methods (NAMs) to access back-end applications.

Web Only Access for SMA supports the following clientless NAM applications:

- Remote Desktop Protocol (RDP)

  ⓘ **NOTE:** On Terminal Server connections, HTML RDP bookmarks are not supported for *per-device* licensing. HTML RDP bookmarks are only supported for *per-user* licensing.

- Secure Shell (SSH)
- Telnet
- Virtual Network Computing (VNC)
- Citrix

ⓘ **NOTE:** SMA 11.3 and higher do not support Java clients, and Java deprecation warnings are shown on AMC screens.

WorkPlace Lite is an access mode for the Secure Mobile Access (SMA) appliance that bypasses all Access and EPC Agents and logs the user in to WorkPlace. The only prerequisite for logging in to a WorkPlace Lite enabled WorkPlace site is that you must use a modern web browser that supports HTML. Web only access is more commonly referred to as Reverse Proxy access.

The AMC administrator can:

- Grant the user access to WorkPlace Lite.
- Force the user to use WorkPlace Lite only.
- Disable the user from accessing WorkPlace Lite.

Users can select a checkbox or go to a specific WorkPlace site for Lite access. If the user checks WorkPlace Lite mode, then the system allows access to browser based graphical and text-terminal shortcuts as well as Web URL and HTML file share shortcuts.

Topics:

- Adding a Text Terminal Shortcut using SSH or Telnet
- Adding a Graphical Terminal Shortcut for a VNC
- Configuring Windows Terminal Services
- Configuring WorkPlace Lite
- TLS and NLA support for HTML RDP

Citrix Configuration

Selecting Citrix from the drop-down menu alters the **Advanced** options menu and pre-populates that section with default settings.

To configure a Citrix server farm:

1. In the **Port** field, type the port number that should be used for Citrix server farm (default **1494** for Citrix).
2. In the **Single Sign-on** section, select how end users will sign on:

   ⓘ | **NOTE:** Single sign-on fields on the **Advanced** page can be completed with absolute values or by clicking the **Variable** button to the right of the field, selecting the desired variable from the displayed list, and clicking **Insert**.

   - **None (prompt user)** - Prompts the end-user for credentials.
   - **Forward user's session credentials** - Uses the user's session credentials (username/password) to login to the backend RDP machine. In the **Domain** field, specify the Windows domain that should be forwarded to the backend RDP machine when attempting to log on.
   - **Forward static credentials** - Defines static credentials (either manually or via policy variables) to be sent to the backend server during the logon request. To forward static credentials, specify the static **Username**, **Password**, and **Domain** to be used.
3. Select the **Enable SSO to Citrix application** checkbox to allow credentials to be submitted to the published applications. The default is off.
4. Select the **Bring remote audio to local computer** checkbox to enable users to access remote audio during the session. The default is off.

   ⓘ | **NOTE:** Audio redirection is network intensive and can affect performance.
5. Select the **Share clipboard between local and remote computers** checkbox to enable clipboard copy/paste in both directions for the user. The default is to allow this feature.
6. To change the **Screen resolution**, select the desired screen resolution from the drop-down menu or select **Custom** and type the custom resolution (default **1024 x 768**). The administrator can also let the Workplace User choose.

7. To change the color depth for the display, select the desired color depth from the **Color Depth** drop-down menu (default **16-bit**).

8. Click **Finish to save the settings, Cancel to delete your entries, or Back to return to the General tab**.

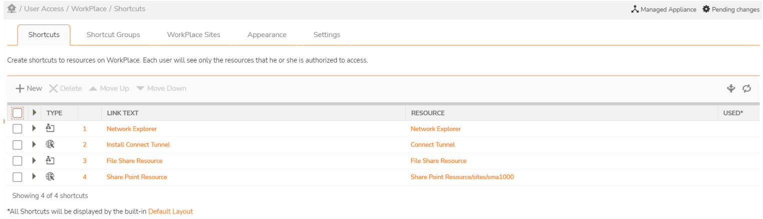
Adding a Text Terminal Shortcut

Use this page to create or edit the text terminal shortcuts appearing in WorkPlace. These shortcuts enable users to easily connect to SSH or Telnet resources.

To add a text terminal shortcut:

1. In the AMC, navigate to **User Access > WorkPlace**.

2. Click on the **Shortcuts** tab.



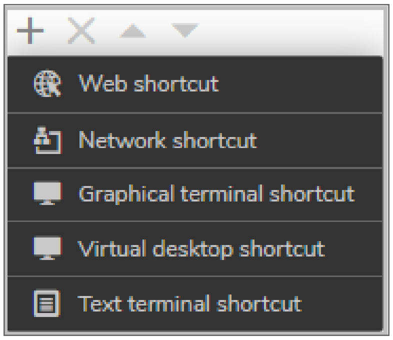
Create shortcuts to resources on WorkPlace. Each user will see only the resources that he or she is authorized to access.

TYPE		LINK TEXT	RESOURCE	USED*
	1	Network Explorer	Network Explorer	
	2	Install Connect Tunnel	Connect Tunnel	
	3	File Share Resource	File Share Resource	
	4	Share Point Resource	Share Point Resource/sites/sma1000	

Showing 4 of 4 shortcuts

*All Shortcuts will be displayed by the built-in Default Layout

3. Click the **+** (New) icon.



4. Select **Text Terminal Shortcut** from the dropdown list.

   The **Add Text Terminal Shortcut** page displays.

5. On the **General** tab, select the resource from the **Resource** drop-down menu.

6. In the **Link Text** field, type in the hyperlink text that will appear as the shortcut for a SSH or Telnet host.

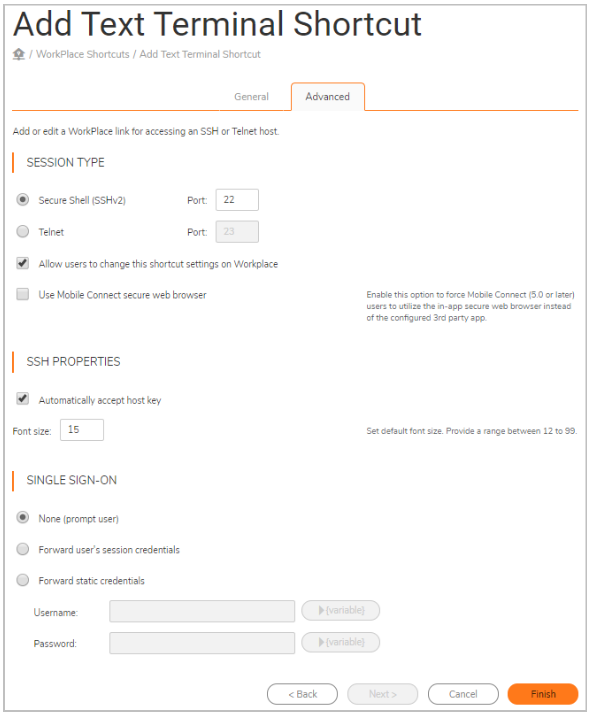
7. Type a description for the shortcut into the **Description** field.

8. In the **Add this shortcut to group** drop-down menu, select **Standalone shortcuts** if you do not want to make this shortcut part of a group, or select an existing group from the list. To create a new group, select **New**.

9. If you selected **New**, type a name for the new group in the **New group name** field.

10. Click **Next**.

The **Advanced** tab displays.



Add Text Terminal Shortcut

/ WorkPlace Shortcuts / Add Text Terminal Shortcut

Add or edit a WorkPlace link for accessing an SSH or Telnet host.

SESSION TYPE

● Secure Shell (SSHv2) Port: 22

○ Telnet Port: 23

☑ Allow users to change this shortcut settings on Workplace

□ Use Mobile Connect secure web browser

Enable this option to force Mobile Connect (5.0 or later) users to utilize the in-app secure web browser instead of the configured 3rd party app.

SSH PROPERTIES

☑ Automatically accept host key

Font size: 15

Set default font size. Provide a range between 12 to 99.

SINGLE SIGN-ON

● None (prompt user)

○ Forward user's session credentials

○ Forward static credentials

Username:

Password:

Fully Customizing WorkPlace Pages

The WorkPlace customization that can be done in AMC (described in Configuring WorkPlace General Settings) are a convenient way to change the general look and feel of WorkPlace, but they may not provide enough control for some deployments.

This section describes two levels of customization:

- WorkPlace style and layout can be configured in AMC, as described in Modifying the Appearance of WorkPlace. To take this customization a step further and, for example, use a background image for your WorkPlace pages, or change the size of the header area, download an existing style, edit it locally, and upload it back up to your appliance. See WorkPlace Style Customization: Manual Edits for more information.
- If you need to do more advanced customization, such as adding a use agreement or end-user license agreement to the login process, you can customize specific pages in WorkPlace, including authentication, error, and notification pages. See About Custom WorkPlace Templates for more information.

Topics:

- WorkPlace Style Customization: Manual Edits
- About Custom WorkPlace Templates
- How Template Files are Matched
- Customizing WorkPlace Templates

WorkPlace Style Customization: Manual Edits

WorkPlace style and layout can be configured in AMC, as described in Modifying the Appearance of WorkPlace. If you are familiar with creating Web content and style sheets (`.css`), you can take this customization a step further and, for example, make your login and logoff pages visually consistent with your corporate standards, or modify the error pages (which appear if a resource is unavailable or a user provides invalid credentials) to include detailed support or troubleshooting information.

The most efficient way to create a new style is to download an existing style, edit it locally, and upload it back up to your appliance.

To fully customize a WorkPlace style:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click the **Appearance** tab.
3. In the **Styles** section, select a style that you want to use as your starting point, and then click **Download**.

   ⓘ | **NOTE:** Styles can be downloaded only one at a time.

   The style is downloaded as a compressed (`.zip`) file, and its filename is a combination of `WorkPlace_Style` followed by the current style name.

   - If you plan to create a new style, rename the `.zip` file when you save it.
   - If you plan to overwrite an existing style with your changes, keep the current filename.
4. Make edits to the cascading style sheets (one for desktop devices and one for mobile devices) and graphics. You can use the sample WorkPlace and login HTML pages to see how page elements are classified.
5. Gather your edits into a `.zip` file name `WorkPlace_Style_<`*`your style name`*`>.zip`, and then click **Upload** on the WorkPlace **Appearance** page.
6. On the **Upload Style** page, select whether you are uploading changes to an existing style, or adding a new WorkPlace style. Uploading a style in the form of a `.zip` file overwrites all style files.
7. If you are uploading a new WorkPlace style, give it a name; for example, *Corporate Branding*.
8. In the **Style zip file** field, enter the name of the `.zip` file you edited or created. If your new style is named *Corporate Branding*, for example, the name of the corresponding file must be *`WorkPlace_Style_Corporate_Branding.zip`*.
9. Click **Upload** to transfer the style-related files to your appliance.

Network Explorer

Network Explorer, available through WorkPlace, is a Web-based user interface that provides access to any shared Windows file system resources a user has permission to access (even from a computer that isn't running Windows). These resources can include domains, servers, computers, workgroups, folders, and files.

Network Explorer is an optional component that can be controlled through policy or completely disabled. It is supported on any browser supported by WorkPlace. For more information, see The WorkPlace Portal.

Tunnel Clients

The Secure Mobile Access tunnel clients provide secure access for TCP and UDP traffic; bi-directional traffic, such as remote Help Desk applications; cross-connections, such as VoIP applications; and reverse connections, such as SMS. The clients all provide network-level access to all resources, effectively making the user's computer a node on your network:

- OnDemand Tunnel agent is a browser-based, Web-activated agent.
- Connect Tunnel client is a Web-installed client. Connect Tunnel may also be installed by an administrator with a file downloaded from AMC. The tunnel clients are managed from the AMC using the network tunnel service. Configuring this service to manage TCP/IP connections from the network tunnel clients requires setting up IP address pools that are used to allocate IP addresses to the clients.

Topics:

- OnDemand Tunnel Agent
- Connect Tunnel Client

OnDemand Tunnel Agent

The OnDemand Tunnel agent enables you to provide complete network and application access through a Web browser to resources protected by the network tunnel service. The OnDemand Tunnel agent provides the same broad application and protocol access as the Connect Tunnel client, but it is integrated into the WorkPlace portal and automatically starts each time users log in to WorkPlace.

The OnDemand Tunnel agent is supported on Windows and macOS.

Connect Tunnel Client

The Connect Tunnel client provides full access to resources protected by the network tunnel service, and to any type of application, including those that use TCP, and non-TCP protocols such as VoIP and ICMP. Connect Tunnel also includes split-tunneling control, granular access controls, proxy detection, and authentication.

The Connect Tunnel client can be deployed in a number of ways (for more information, see Client Installation Packages):

- Offer users a shortcut in WorkPlace for downloading and installing the client; the link points to the *Connect Tunnel* resource, described in Built-In Resources.
- If you don't want to require users to log in to WorkPlace, have them download and install the Connect Tunnel client components from a network location (such as a Web server, FTP server, or file server).
- Distribute installation packages using an application such as SMS or Tivoli.
- Create a master image of a Connect Tunnel install and copy it to user systems using a third-party disk-image copying utility such as Norton Ghost.

The Connect Tunnel client is supported on Windows, Linux, and MacOS operating systems, and installation of the Connect Tunnel client requires users to have administrator privileges. All Connect Tunnel configuration and management is performed in AMC.

When Connect Tunnel is active, a **Connect Tunnel** icon is displayed in the system task bar.

You can configure the Windows version of the Connect Tunnel client software to be automatically updated on users' computers whenever a new version becomes available. For more information, see Windows Tunnel Client Automatic Client Updating.

Web Access

This section provides an overview of the zero-client Web access methods such as translated Web access, custom port mapped Web access, and custom FQDN mapped Web access. A section describing Exchange ActiveSync Web access is also included.

Topics:

- WorkPlace Lite
- Translated ActiveSync Web Access
- Custom Port Mapped Web Access
- Custom FQDN Mapped Web Access
- Notes for Custom Port Mapped or Custom FQDN Mapped Web Access
- Seamless Editing in SharePoint
- Exchange ActiveSync access
- ActiveSync Resource Configuration with SAN Certificates
- Outlook Anywhere Web Access

WorkPlace Lite

WorkPlace Lite is an access mode for the SMA appliance that bypasses all Access and EPC Agents and logs the user in to WorkPlace. The only prerequisite for logging into a WorkPlace Lite-enabled WorkPlace site is a modern web browser. Web only access is more commonly referred to as Reverse Proxy access.

Translated ActiveSync Web Access

Translated Web provides basic access to Web resources, and enables you to create aliases that obscure internal host names. It proxies Web content directly through the appliance and provides access to any Web resource that is specifically configured to run with WorkPlace, as well as access to Windows network shares. Translated Web access works on any Web browser that supports SSL and has JavaScript enabled. It uses URL rewriting, which may have limitations with some Web applications, such as JavaScript. Custom port mapping or custom FQDN mapping may be used as an alternative to URL translation.

Custom Port Mapped Web Access

Custom port mapping involves mapping the backend resource or server to a port number at the SMA appliance. The application listens on this port and all HTTPS traffic received on it is terminated at the appliance. A new HTTP request is made to retrieve the mapped backend resource. The HTTP reply is transmitted using plain text to facilitate translation of absolute URLs. URL rewriting is not used. When using custom port mapping, any firewalls in the network must be configured to keep the specific ports open. Custom port mapping does not require installation of a client agent, and works with any Web browser.

Custom FQDN Mapped Web Access

Custom FQDN mapping means that the backend resource or server is mapped to an external fully qualified domain name (host and domain). The resource should be accessed with the FQDN name rather than with the IP address. The FQDN name should be resolvable to an IP address in the public domain. The application listens on port 443 at this IP address. All HTTPS traffic is terminated at this socket. A new HTTP request is made to retrieve the mapped backend resource. The HTTP reply is transmitted using plain text to facilitate translation of absolute URLs. URL rewriting is not used.

Notes for Custom Port Mapped or Custom FQDN Mapped Web Access

These access methods are ideal for all well written applications that predominantly use relative URLs. JavaScript may also behave better with these access methods than the Translated Web Access.

The following applications are recommended for Custom Port Mapped or Custom FQDN Mapped Web Access over Translated Web Access:

- Share Point2010, SharePoint 2013, SharePoint 2016
- Outlook Web Access 2013, Outlook Web Access 2016
- Domino Web Access
- Complex web applications (JavaScript/other advanced web technologies)

Topics:

- Configuration Requirements
- Known Behavior

Configuration Requirements

- Each resource should be configured using only one of the access methods. Do not mix translated, custom port mapped and custom FQDN-mapped modes.
- Do not include a path in the URL. For example, do not use a URL like:

  ```
  http(s)://backend_hostname(:portNumber)
  ```

  To set the complete path on WorkPlace, specify the start page on the Edit WorkPlace ShortCuts > Advanced page, as explained in Adding Web Shortcuts.

- Use of valid Certificates is highly recommended.
    - Single sign-on for the appliance might not work with Internet Explorer when a custom FQDN mapped resource with an invalid certificate is accessed from WorkPlace. For example, this could happen when a user logs in to WorkPlace and clicks a custom FQDN mapped resource that has a self-signed certificate or otherwise does not have a valid certificate on the appliance. A JavaScript certificate warning is popped up to the Internet Explorer user. After the user accepts the certificate, Internet Explorer does not transmit the “referrer” HTTP header to the initial page. This referrer value is required for single sign-on functionality. This issue does not occur when using browsers other than Internet Explorer, or when there is no certificate warning, or when wildcard or SAN certificates are used.
    - Custom Port Mapped resource may get redirected to Workplace Portal in case of certificate warning while accessing with Internet Explorer.
- The resources should be configured and accessed using host and domain name only, not via IP address.

Known Behavior

Logging out of applications like OWA and SharePoint from an Internet Explorer browser may log you out of Workplace.

ⓘ **NOTE:** Logging out does not affect other active WorkPlace shortcut sessions. Only the browser is logged off as the backend application clears all cookies (including appliance-specific cookies) on logoff.

Seamless Editing in SharePoint

The SonicWall Secure Mobile Access (SMA) platform supports Microsoft SharePoint access using reverse proxy, as well as seamless editing of Office documents while in SharePoint. SMA accomplishes this by allowing persistent cookie information to be stored on appropriate zones. Administrators can enable or disable persistent cookie information on the user’s system.

ⓘ **NOTE:** Editing SharePoint documents from a zone that allows persistent session storage is available only for Microsoft Internet Explorer (IE).

ⓘ **NOTE:** In cases where legal regulations require the consent of the user before storing persistent cookies, the Administrator can create an Acceptable Use Policy (AUP).

ⓘ **NOTE:** If a user goes to unsafe zones such as kiosk zones and more, the persistent cookies will not be enabled..

Configuring seamless editing in SharePoint is done in three parts:

- Enabling Storage of Persistent Session Information
- Configuring a Resource as a SharePoint Web Service
- Modifying a Zone to Allow Storing of Persistent Session Information

Enabling Storage of Persistent Session Information

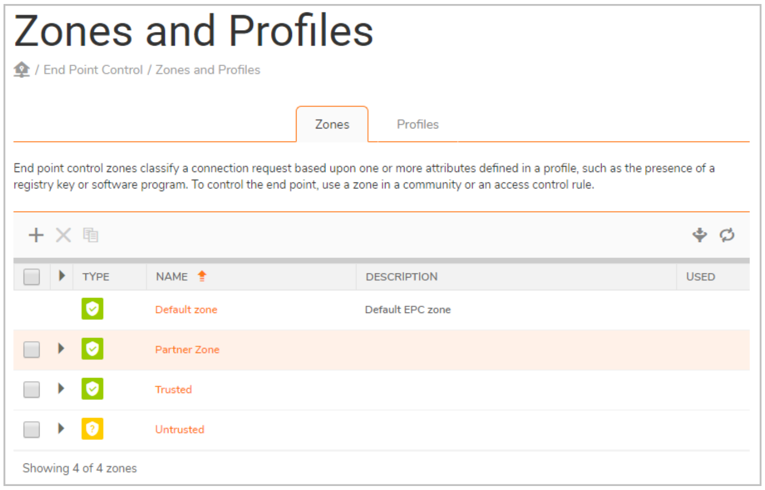
To enable Persistent Cookie information on a user's system:

1. In the AMC, navigate to **User Access > End Point Control**.

   The **End Point Control** page displays.

2. In the **Zones and Profiles** section, click **Edit** next to **Zones**.

   The **Zones and Profiles** page displays.



Zones and Profiles

/ End Point Control / Zones and Profiles

End point control zones classify a connection request based upon one or more attributes defined in a profile, such as the presence of a registry key or software program. To control the end point, use a zone in a community or an access control rule.

□	▸	TYPE	NAME	DESCRIPTION	USED
		✓	Default zone	Default EPC zone	
□	▸	✓	Partner Zone		
□	▸	✓	Trusted		
□	▸	?	Untrusted		

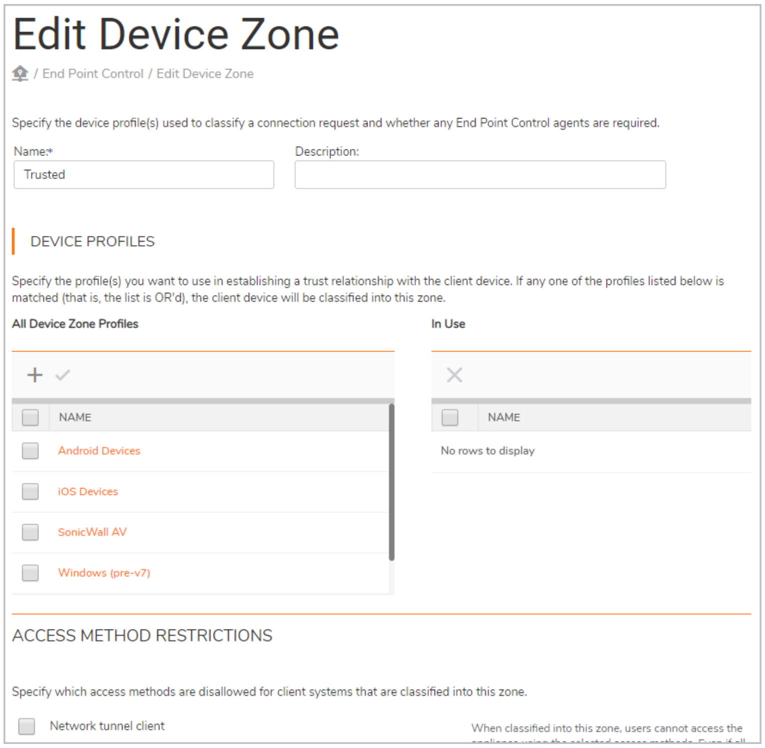
Showing 4 of 4 zones

3. Select a zone or create a new zone as follows:

   a. If you want a new zone, see Creating a Device Zone.

   b. If you want to change one of the existing zones, click on that zone in the table.

   The **Edit Device Zone** page displays.



Edit Device Zone

/ End Point Control / Edit Device Zone

Specify the device profile(s) used to classify a connection request and whether any End Point Control agents are required.

Name:* Trusted

Description:

DEVICE PROFILES

Specify the profile(s) you want to use in establishing a trust relationship with the client device. If any one of the profiles listed below is matched (that is, the list is OR'd), the client device will be classified into this zone.

All Device Zone Profiles

□	NAME
□	Android Devices
□	iOS Devices
□	SonicWall AV
□	Windows (pre-v7)

In Use

□	NAME
	No rows to display

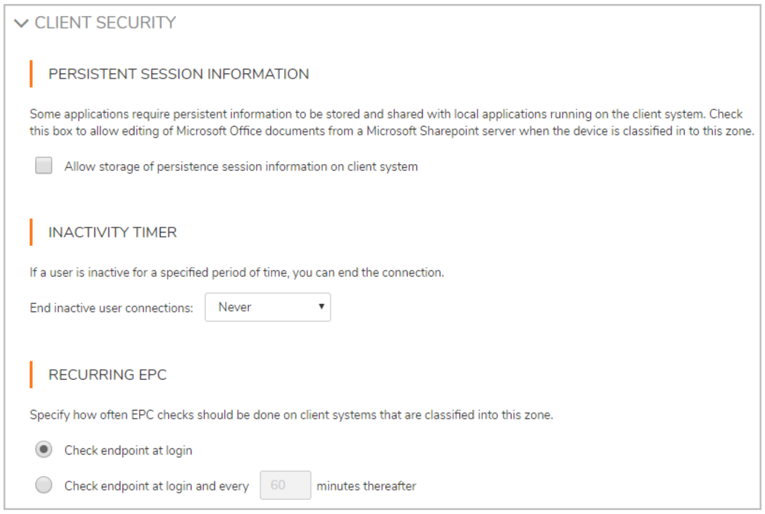
ACCESS METHOD RESTRICTIONS

Specify which access methods are disallowed for client systems that are classified into this zone.

□ Network tunnel client

When classified into this zone, users cannot access the appliance using the selected access methods. Even if all

4. Scroll down to the **Client Security** section and expand it.



CLIENT SECURITY

PERSISTENT SESSION INFORMATION

Some applications require persistent information to be stored and shared with local applications running on the client system. Check this box to allow editing of Microsoft Office documents from a Microsoft Sharepoint server when the device is classified in to this zone.

□ Allow storage of persistence session information on client system

INACTIVITY TIMER

If a user is inactive for a specified period of time, you can end the connection.

End inactive user connections: Never

RECURRING EPC

Specify how often EPC checks should be done on client systems that are classified into this zone.

● Check endpoint at login

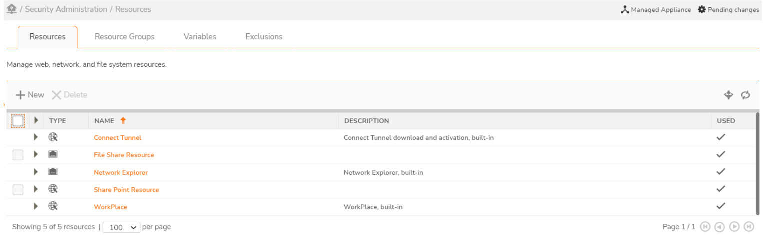
○ Check endpoint at login and every 60 minutes thereafter

5. In the **Persistent Session Information** section, select **Allow storage of persistence session information on client system**.

Configuring a Resource as a SharePoint Web Service

To configure a resource as a SharePoint Web Service:

1. In the AMC, navigate to **Security Administration > Resources**.

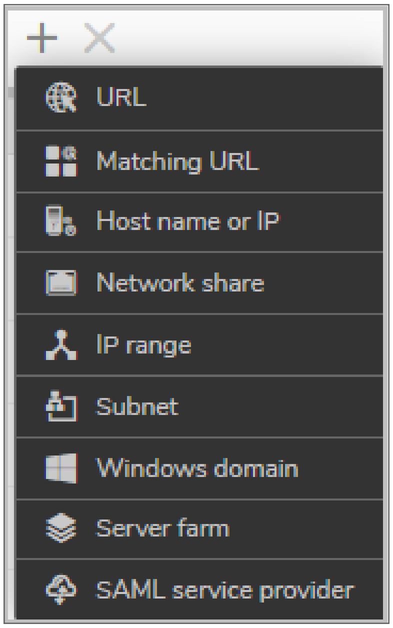
   Manage web, network, and file system resources.

TYPE	NAME	DESCRIPTION	USED
	Connect Tunnel	Connect Tunnel download and activation, built-in	✓
	File Share Resource		✓
	Network Explorer	Network Explorer, built-in	✓
	Share Point Resource		✓
	WorkPlace	WorkPlace, built-in	✓

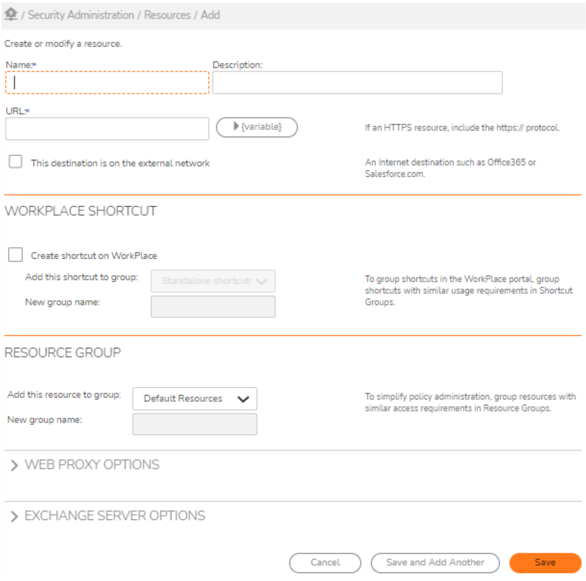
   Showing 5 of 5 resources | 100 per page   Page 1 / 1

2. Click click the **+** (New) icon.

3. Select **URL** from the drop-down list.

   The **Add Resource - URL** page displays.



/ Security Administration / Resources / Add

Create or modify a resource.

Name:*

Description:

URL:*

If an HTTPS resource, include the https:// protocol.

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUT

□ Create shortcut on WorkPlace

Add this shortcut to group: Standalone shortcut

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

RESOURCE GROUP

Add this resource to group: Default Resources

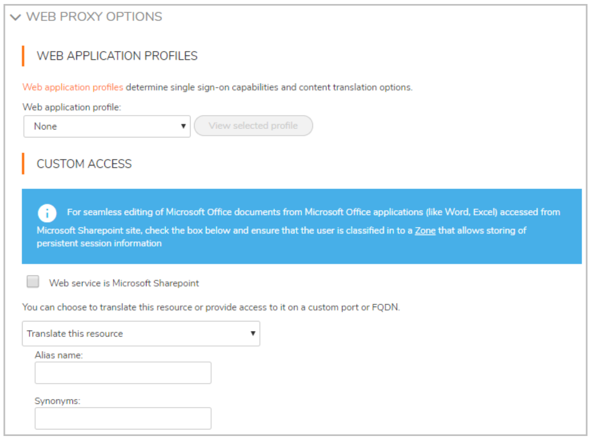
New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

> WEB PROXY OPTIONS

> EXCHANGE SERVER OPTIONS

4. Enter the **Name** and the **URL** for this resource.
5. If this resource is on the external network, select the checkbox for **This destination is on the external network**.
6. Scroll down to the **Web Proxy Options** section and expand it.



WEB PROXY OPTIONS

WEB APPLICATION PROFILES

Web application profiles determine single sign-on capabilities and content translation options.

Web application profile: None

CUSTOM ACCESS

For seamless editing of Microsoft Office documents from Microsoft Office applications (like Word, Excel) accessed from Microsoft Sharepoint site, check the box below and ensure that the user is classified in to a Zone that allows storing of persistent session information

□ Web service is Microsoft Sharepoint

You can choose to translate this resource or provide access to it on a custom port or FQDN.

Translate this resource

Alias name:

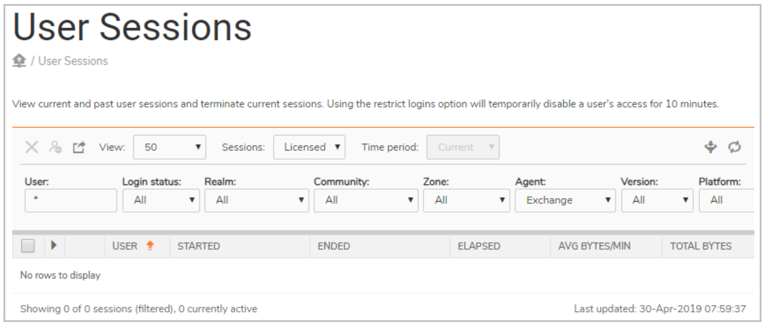
Synonyms:

7. From the **Web application profile** drop-down menu, select **SharePoint.**
8. Select the **Web service is Microsoft Sharepoint** checkbox.
9. Select **Access this from resource using a custom FQDN**.
10. In the **Custom FQDN** field, enter the FQDN.

Modifying a Zone to Allow Storing of Persistent Session Information

To modify a zone to allow storing of persistent session information on a client system:

1. In the AMC, navigate to **Monitoring > User Sessions**.



User Sessions

/ User Sessions

View current and past user sessions and terminate current sessions. Using the restrict logins option will temporarily disable a user's access for 10 minutes.

View: 50 Sessions: Licensed Time period: Current

User:	Login status:	Realm:	Community:	Zone:	Agent:	Version:	Platform:
*	All	All	All	All	Exchange	All	All

	USER	STARTED	ENDED	ELAPSED	AVG BYTES/MIN	TOTAL BYTES

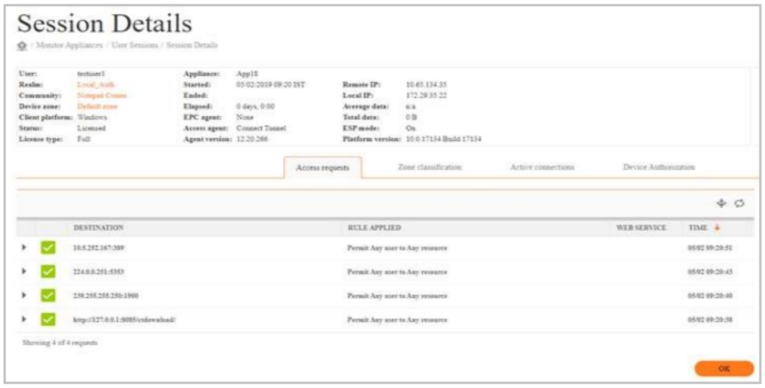
No rows to display

Showing 0 of 0 sessions (filtered), 0 currently active

Last updated: 30-Apr-2019 07:59:37

2. Click on the User Session that you want.

   The **Session Details** page displays.



Session Details

/ Monitor Appliances / User Sessions / Session Details

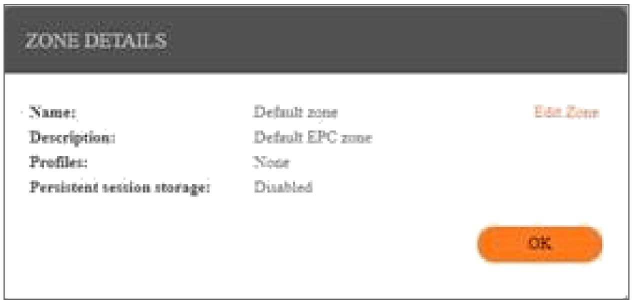
User:	testuser1	Appliance:	App18		
Realm:	Local_Auth	Started:	05/02/2019 09:20 IST	Remote IP:	10.65.134.35
Community:	Notepad Comm	Ended:		Local IP:	172.29.35.22
Device zone:	Default zone	Elapsed:	0 days, 0:00	Average data:	n/a
Client platform:	Windows	EPC agent:	None	Total data:	0 B
Status:	Licensed	Access agent:	Connect Tunnel	ESP mode:	On
License type:	Full	Agent version:	12.20.266	Platform version:	10.0.17134 Build 17134

		DESTINATION	RULE APPLIED	WEB SERVICE	TIME
▸	☑	10.5.252.167:389	Permit Any user to Any resource		05/02 09:20:51
▸	☑	224.0.0.251:5353	Permit Any user to Any resource		05/02 09:20:43
▸	☑	239.255.255.250:1900	Permit Any user to Any resource		05/02 09:20:40
▸	☑	http://127.0.0.1:8085/cxdownload/	Permit Any user to Any resource		05/02 09:20:38

Showing 4 of 4 requests

3. Click on the zone that you want.

   The **Zone Details** dialog displays.

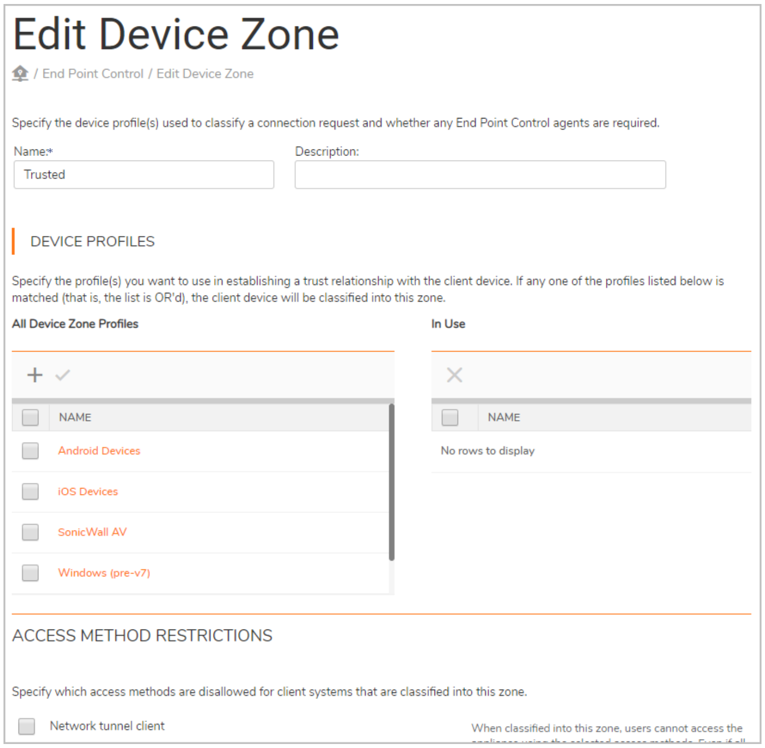


ZONE DETAILS

Name:	Default zone	Edit Zone
Description:	Default EPC zone	
Profiles:	None	
Persistent session storage:	Disabled	

4. Click **Edit Zone**.

   The **Edit Device Zone** page displays.



Edit Device Zone

/ End Point Control / Edit Device Zone

Specify the device profile(s) used to classify a connection request and whether any End Point Control agents are required.

Name:* Trusted

Description:

DEVICE PROFILES

Specify the profile(s) you want to use in establishing a trust relationship with the client device. If any one of the profiles listed below is matched (that is, the list is OR'd), the client device will be classified into this zone.

All Device Zone Profiles

□	NAME
□	Android Devices
□	iOS Devices
□	SonicWall AV
□	Windows (pre-v7)

In Use

□	NAME
	No rows to display

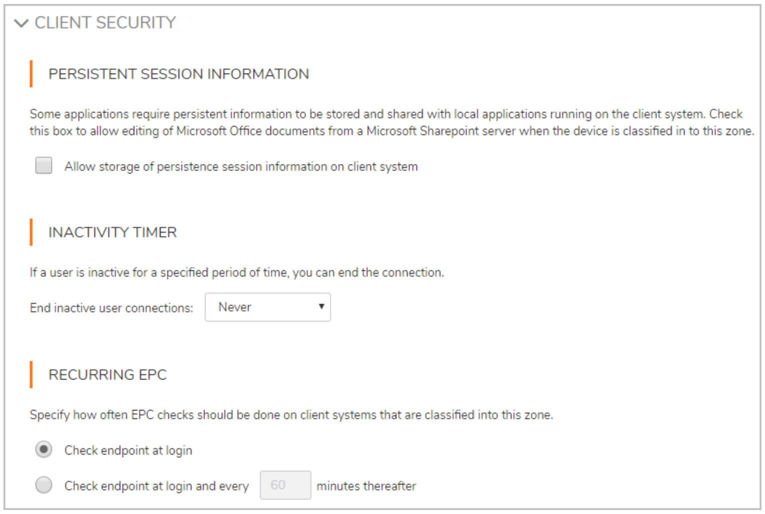
ACCESS METHOD RESTRICTIONS

Specify which access methods are disallowed for client systems that are classified into this zone.

□ Network tunnel client

When classified into this zone, users cannot access the

5. Scroll down to the **Client Security** panel and open it.



CLIENT SECURITY

PERSISTENT SESSION INFORMATION

Some applications require persistent information to be stored and shared with local applications running on the client system. Check this box to allow editing of Microsoft Office documents from a Microsoft Sharepoint server when the device is classified in to this zone.

□ Allow storage of persistence session information on client system

INACTIVITY TIMER

If a user is inactive for a specified period of time, you can end the connection.

End inactive user connections: Never

RECURRING EPC

Specify how often EPC checks should be done on client systems that are classified into this zone.

● Check endpoint at login

○ Check endpoint at login and every 60 minutes thereafter

6. Under **Persistent session information**, select the **Allow storage of persistence session information on client system** checkbox.

Exchange ActiveSync access

Secure Mobile Access supports Exchange ActiveSync for Apple iPhones/iPads and smart phones or tablets that run the Android 7.x or 8.x operating system.

After the administrator configures the SMA appliance, a user with a supported smart phone or tablet can configure the device to access email using Exchange ActiveSync.

To do this, the user enters an email account name, server, domain, user name and password. The user turns on ActiveSync for this account. The results are saved as a new email account on the device.

With ActiveSync turned on, the device gives the user notice when new mail arrives.

When the user syncs the iPhone to a computer that is connected to the Exchange server through the SMA appliance, the mail, contacts and calendar are updated.

Topics:

- Enabling Exchange ActiveSync access on the appliance
- Exchange ActiveSync sessions
- Notes for Exchange ActiveSync device profiles

Enabling Exchange ActiveSync access on the appliance

The administrator can enable Exchange ActiveSync access for a community of iPhone or Android device users. This involves the following tasks:

- Create a realm that uses an Active Directory authentication server. Realms that use chained authentication are not supported for Exchange ActiveSync.
- Create a resource for Exchange ActiveSync using the **Exchange Server Options** section of the **Add Resource** page for a URL resource.

  The **Exchange Server Options** section allows the administrator to specify a custom FQDN, IP address, SSL certificate, and realm to use for providing Exchange ActiveSync access.

  The custom FQDN, IP address, and SSL certificate options function in the same way as those for Workplace sites that use these options. The custom FQDN provides a host/domain name through which ActiveSync connections or sessions can be established.

  The IP address is a virtual IP address hosted by the appliance, and must be on the same subnet as the external interface (or the internal if single-homed) of the SMA appliance so that it is reachable via the public interface of the appliance.

  The SSL certificate can be a wildcard certificate or you can configure a server certificate that matches the host name.

  The only realms that appear in the Realm drop-down menu are those that use an Active Directory authentication server. Realms that use chained authentication do not appear in the menu. A realm used for Exchange ActiveSync cannot be changed to provide chained authentication or to use an authentication server other than Active Directory.
- Define a Device Profile for end point control of Exchange ActiveSync devices from the **EPC** page in AMC. You can select Exchange ActiveSync as the device profile type.

  The only attribute that can be configured for this device profile is **Equipment ID**. The device serial number is used as the identifier. Equipment ID retrieval uses the underlying operating system hard disk drivers. All driver updates should be applied to ensure that Equipment ID retrieval works reliably.

  The Exchange ActiveSync device profile can be included in any zone for evaluation.

ⓘ **NOTE:** ActiveSync clients will not be able to connect on zones that have Device authorization enabled.

- View the **Network Settings** page to see all custom IP addresses used for virtual hosting, the FQDNs that listen on these addresses, and the associated Resources or WorkPlace Sites.

  The **Resources** and **WorkPlace Site** items are links to the configuration page for easy navigation and editing.
- View the **User Sessions** page, which displays Exchange ActiveSync sessions as belonging to the Exchange ActiveSync Access Agent. **Exchange ActiveSync** is an option in the **Agent** list under **Filters**.

Exchange ActiveSync sessions

Initial connections to the ActiveSync Exchange Server FQDN name cause a username and password challenge by the appliance.

If the user successfully authenticates, the ActiveSync session is established with the Exchange server without further user interaction.

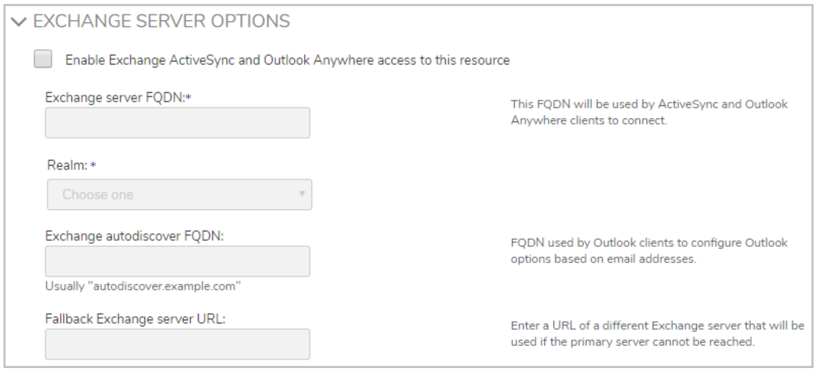
Authentication methods from the appliance to the Exchange server use basic authentication.

Notes for Exchange ActiveSync device profiles

- Device authorization is not supported by ActiveSync clients. ActiveSync clients will not be able to connect on zones that have Device authorization enabled.
- The profiles only work with an ActiveSync stream because that is the only way to obtain the device value.
- Only ActiveSync for Exchange is supported in this release.

ActiveSync Resource Configuration with SAN Certificates

SAN certificates can be used for different host names on the same IP address.On the **Add Resource - URL**> **Exchange Server Options** page, enter the FQDN name in **Exchange Server FQDN** to connect ActiveSync and Outlook Anywhere clients.



EXCHANGE SERVER OPTIONS

□ Enable Exchange ActiveSync and Outlook Anywhere access to this resource

Exchange server FQDN:*

This FQDN will be used by ActiveSync and Outlook Anywhere clients to connect.

Realm: *

Choose one

Exchange autodiscover FQDN:

Usually "autodiscover.example.com"

FQDN used by Outlook clients to configure Outlook options based on email addresses.

Fallback Exchange server URL:

Enter a URL of a different Exchange server that will be used if the primary server cannot be reached.

Outlook Anywhere Web Access

SMA supports Outlook Anywhere (OWA) for Microsoft Outlook clients on Windows. After the administrator configures the SMA appliance, a user can configure the Microsoft Outlook Client to access Emails using Outlook Anywhere and can use the Out-of-Office service as well.

ⓘ **NOTE:** The X-Forwarded-For (XFF) HTTP header field indicates the originating IP address of a client that connects to a web server through an HTTP proxy or load balancer. Extra-webaccess service sends X-Forwarded-For header on all requests to resource or backend servers.

Client Installation Packages

You can make the Connect Tunnel client components available for users to download and install from another network location (such as a Web server, FTP server, or file server) without requiring them to log in to WorkPlace. You can also push the Connect Tunnel client installation package to users through an application such as Tivoli or SMS, or create a master image of a client install and copy it to user systems using a third-party disk-image copying utility.

The client setup packages are available for you to download from AMC. With the Windows-based packages (Connect Tunnel for Windows), you also have the option of configuring various client settings in an `.ini` configuration file before distributing the client to users.

ⓘ **NOTE:** The easiest way to ensure that users are running the latest version is to make client updates automatic; see Windows Tunnel Client Automatic Client Updating for more information.

Topics:

- Downloading the Secure Mobile Access Client Installation Packages

Downloading the Secure Mobile Access Client Installation Packages

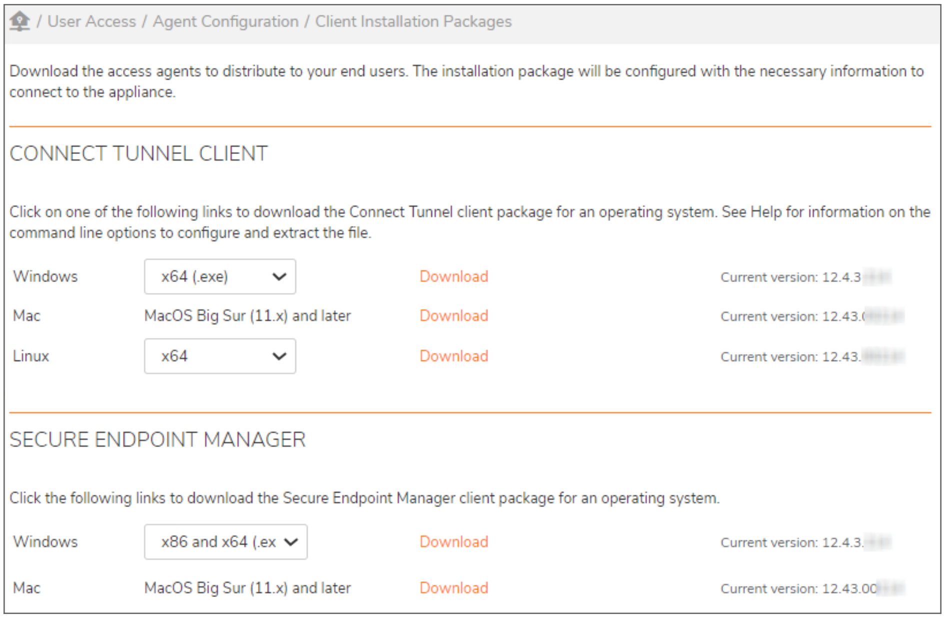
ⓘ **NOTE:** The Legacy Connect Tunnel and Connect Tunnel Service (CTS) are deprecated from 12.4.1 onwards

This section describes how to download the installation package for the Connect Tunnel client to your local workstation.

To download a client installation package:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. In the **Access Agents** section, next to **Client installation packages**, click **Download**.

   The **Client Installation Packages** page displays.



/ User Access / Agent Configuration / Client Installation Packages

Download the access agents to distribute to your end users. The installation package will be configured with the necessary information to connect to the appliance.

CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	x64 (.exe)	Download	Current version: 12.4.3[redacted]
Mac	MacOS Big Sur (11.x) and later	Download	Current version: 12.43.[redacted]
Linux	x64	Download	Current version: 12.43.[redacted]

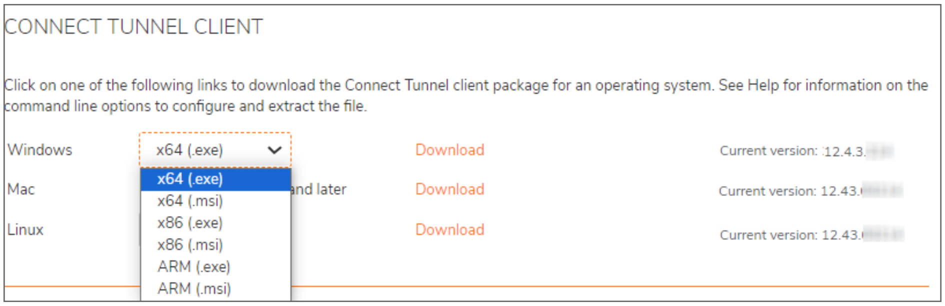
SECURE ENDPOINT MANAGER

Click the following links to download the Secure Endpoint Manager client package for an operating system.

Windows	x86 and x64 (.ex	Download	Current version: 12.4.3.[redacted]
Mac	MacOS Big Sur (11.x) and later	Download	Current version: 12.43.00[redacted]

3. Download the client according to your Operating System:

    - **Windows**: In the Connect Tunnel Client group, click the drop-down next to Windows option and select the installation package based on your operating system. Connect Tunnel for Windows is supported on platforms such as x86, x64, and ARM processor.
    - The available options are:
    - x64 (.exe)
    - x64 (.msi)
    - x86 (.exe)
    - x86 (.msi)
    - ARM (.exe)
    - ARM (.msi)



CONNECT TUNNEL CLIENT

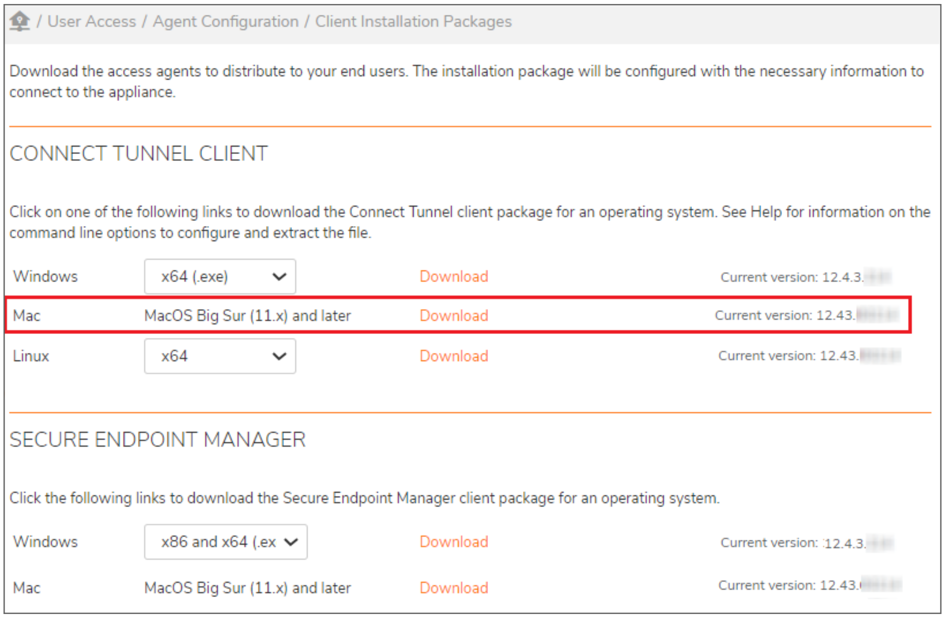
Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	x64 (.exe)	Download	Current version: 12.4.3.[redacted]
Mac	nd later	Download	Current version: 12.43.[redacted]
Linux		Download	Current version: 12.43.[redacted]

NOTE: Connect Tunnel and WorkPlace automatically detects and reports processor architecture (x84, x64, and arm64) to the server. The server then tracks the architecture type in the user session state and installs or updates the platforms automatically.

- **Mac**:In the **Connect Tunnel Client** group, click **Download** next to Mac option.

  ⓘ **NOTE:** Connect Tunnel client is built as universal application which can be run on both Intel and Apple Silicon Mac computers.



/ User Access / Agent Configuration / Client Installation Packages

Download the access agents to distribute to your end users. The installation package will be configured with the necessary information to connect to the appliance.

CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

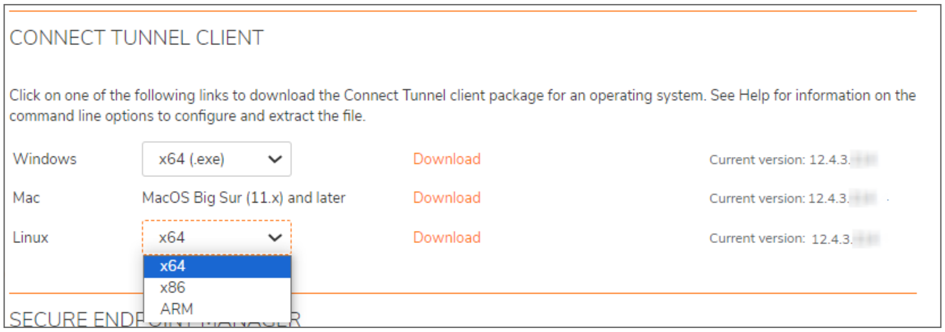
Windows	x64 (.exe)	Download	Current version: 12.4.3.[redacted]
Mac	MacOS Big Sur (11.x) and later	Download	Current version: 12.43.[redacted]
Linux	x64	Download	Current version: 12.43.[redacted]

SECURE ENDPOINT MANAGER

Click the following links to download the Secure Endpoint Manager client package for an operating system.

Windows	x86 and x64 (.ex	Download	Current version: 12.4.3.[redacted]
Mac	MacOS Big Sur (11.x) and later	Download	Current version: 12.43.[redacted]

- **Linux** : In the **Connect Tunnel Client** group, select the installation package based on your operating system from the drop-down menu next to **Linux** option.
  - The available options are:
  - x64
  - x86
  - ARM



CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	x64 (.exe)	Download	Current version: 12.4.3.[redacted]
Mac	MacOS Big Sur (11.x) and later	Download	Current version: 12.4.3.[redacted]
Linux	x64	Download	Current version: 12.4.3.[redacted]

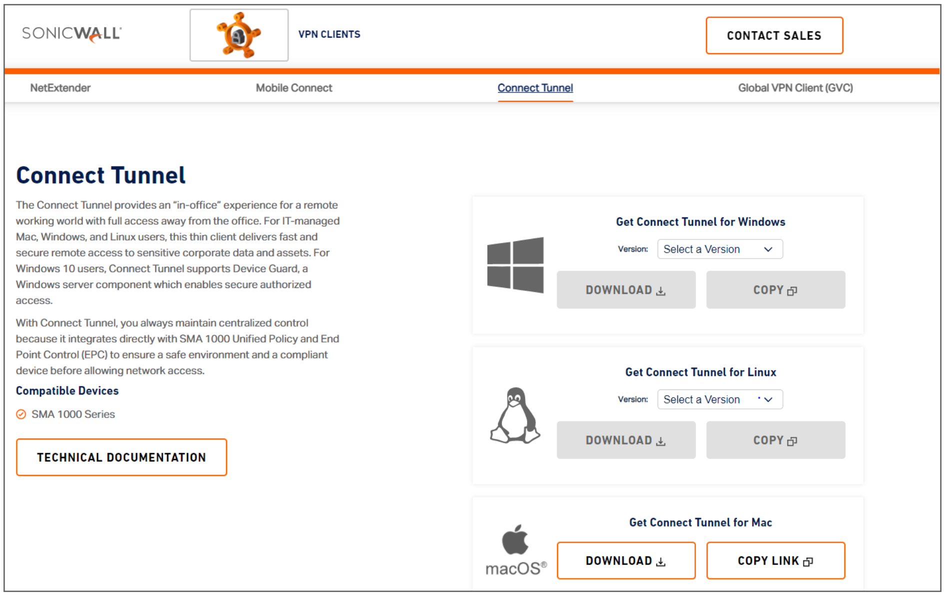
4. Click **Download**.

   The install package is downloaded to your machine.

5. Open the downloaded file and click **Agree** to agree to the terms, then click **Install**.

To download a client installation package from SonicWall website:

1. Browse to https://www.sonicwall.com/products/remote-access/vpn-clients/.
2. Select **Connect Tunnel** tab and download the desired version of Connect Tunnel client based on your operating system.



Connect Tunnel

The Connect Tunnel provides an "in-office" experience for a remote working world with full access away from the office. For IT-managed Mac, Windows, and Linux users, this thin client delivers fast and secure remote access to sensitive corporate data and assets. For Windows 10 users, Connect Tunnel supports Device Guard, a Windows server component which enables secure authorized access.

With Connect Tunnel, you always maintain centralized control because it integrates directly with SMA 1000 Unified Policy and End Point Control (EPC) to ensure a safe environment and a compliant device before allowing network access.

Compatible Devices

SMA 1000 Series

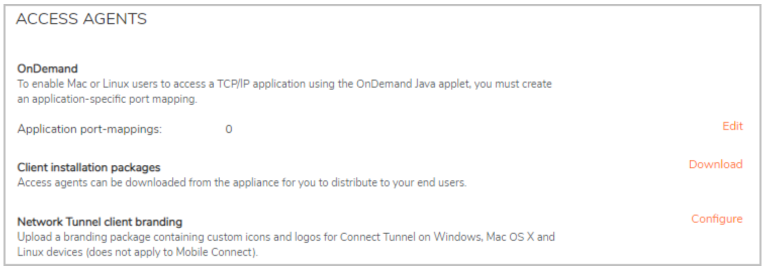
TECHNICAL DOCUMENTATION
Get Connect Tunnel for Windows
Version: Select a Version
DOWNLOAD
COPY
Get Connect Tunnel for Linux
Version: Select a Version
DOWNLOAD
COPY
Get Connect Tunnel for Mac
macOS®
DOWNLOAD
COPY LINK

Network Tunnel Client Branding

Custom branding is available for the Connect Tunnel user interface. This feature allows companies to replace the SonicWall branding in Connect Tunnel windows with their own company names and logos. Connect Tunnel branding is available on Windows, macOS, and Linux platforms and is done on a per-appliance basis.

To upload customized branding graphics and guidelines:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. Next to **Network Tunnel client branding**, click **Configure**.



ACCESS AGENTS

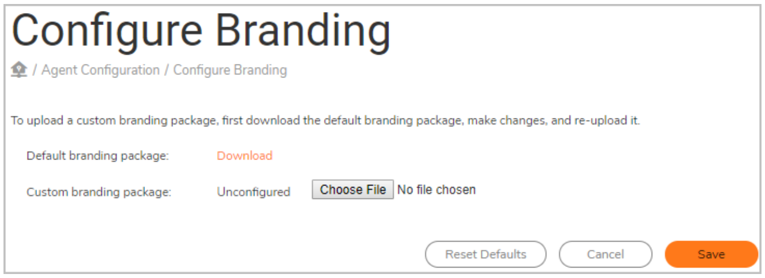
OnDemand
To enable Mac or Linux users to access a TCP/IP application using the OnDemand Java applet, you must create an application-specific port mapping.

Application port-mappings: 0

Client installation packages
Access agents can be downloaded from the appliance for you to distribute to your end users.

Network Tunnel client branding
Upload a branding package containing custom icons and logos for Connect Tunnel on Windows, Mac OS X and Linux devices (does not apply to Mobile Connect).

3. Click **Download** next to **Default branding package** and select the download location.



Configure Branding

/ Agent Configuration / Configure Branding

To upload a custom branding package, first download the default branding package, make changes, and re-upload it.

Default branding package: Download

Custom branding package: Unconfigured Choose File No file chosen

4. Click **OK** to return to the **Configure Branding** page.
5. Unzip the downloaded file, which contains a folder of branding files for each platform (Windows, Linux, and Mac). Using the `README.txt` file as a guide, replace the default files with custom branding files, and then zip the files.
6. On the **Configure Branding** page, click the **Browse** button and select the zip file containing the custom branding files.
7. After saving the file, click **Save**.

   All Connect Tunnel windows and icons are then updated with custom branding.

The OnDemand Proxy Agent

The OnDemand Proxy Agent is a secure, lightweight agent that provides access to TCP/IP resources. It uses local loopback proxying to redirect communication to protected network resources according to routing directives defined in AMC (it does not support UDP applications).

Note that the OnDemand Proxy Agent does not scale as effectively as the OnDemand Tunnel agent. The OnDemand Proxy Agent is not recommended for usage as a broad VPN agent, but instead should be targeted for access to specific applications through WorkPlace. In situations where you want to provide broad access to applications through the WorkPlace portal for more than 500 concurrent users at a time, we recommend that you deploy the OnDemand Tunnel agent instead. Note that you can use OnDemand Proxy as a fallback for OnDemand Tunnel in case OnDemand Tunnel cannot be installed (perhaps due to issues around administrative rights). In that scenario, you would configure both OnDemand Tunnel and OnDemand Proxy within a community.

This section provides an overview of OnDemand and describes how to configure and deploy it.

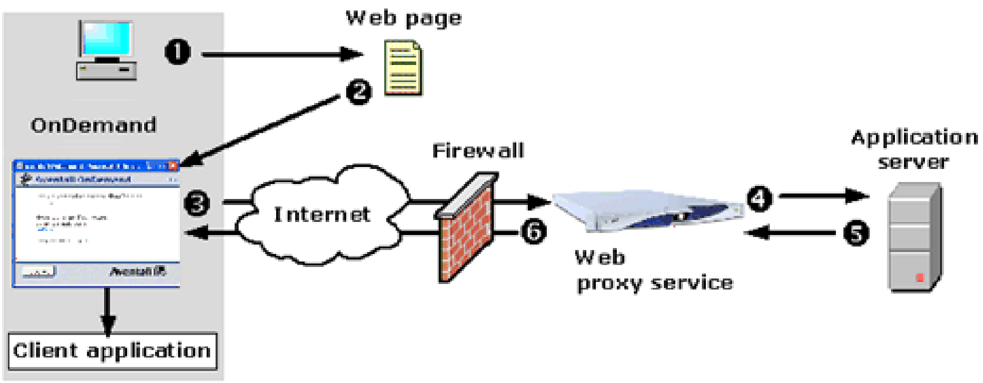
Topics:

- About OnDemand Proxy
- How OnDemand Redirects Network Traffic
- Configuring OnDemand to Access Specific Applications
- Client Configuration

About OnDemand Proxy

OnDemand Proxy is a loopback-based proxy solution that secures communication between a client application and an application server. The below image illustrates the connection sequence.

OnDemand Proxy Connection Sequence



1. OnDemand starts automatically when the user logs in to WorkPlace.
2. OnDemand runs within the WorkPlace window.
3. OnDemand waits for application requests on the local loopback address (`127.0.0.1`) and redirects the traffic to the Web proxy service.
4. The Web proxy service proxies the traffic to an application server using the application's required port(s).
5. The application server sends application traffic to the Web proxy service.
6. The Web proxy service sends the application traffic to OnDemand, which then passes it to the client application.

OnDemand supports TCP applications that use one or multiple ports, including applications that dynamically define ports (it does not support UDP-based applications). The below table lists applications typically accessed using OnDemand.

Applications Accessed Using OnDemand

Application	Examples

Resident client/server Typically, these client applications are installed locally on the client computer	Internet email applications: • Microsoft Outlook • Outlook Express • Lotus Notes • Netscape Mail • Eudora Terminal emulation applications: • NetManage RUMBA PC-to-Host Remote office connectivity applications: • Citrix ICA/Xenapp • Microsoft Windows Terminal Services

By default, OnDemand is configured to run automatically when the user connects to WorkPlace. For optimum performance, OnDemand is installed on the user's computer the first time it is accessed, minimizing download time for returning users.

Topics:

- OnDemand Mapped Mode
- Activating OnDemand

OnDemand Mapped Mode

By default, OnDemand starts automatically when users log in to WorkPlace. Mapped mode enables users to click a shortcut that is configured for a specific application. Optionally, you can configure OnDemand to automatically launch a specified Web URL when users click a shortcut. This is useful for starting an application (such as a thin-client application) when OnDemand runs. You must manually create any shortcuts to specific applications. Mapped mode is supported on Windows, MacOS, and Linux platforms.

On Windows PCs, when a user logs in to WorkPlace for the first time, WorkPlace automatically downloads, installs, and launches OnDemand on the user's computer (assuming the community the user belongs to is configured to do so). On subsequent WorkPlace logins, WorkPlace automatically starts OnDemand.

Activating OnDemand

By default, when OnDemand is enabled, it starts automatically when users log in to WorkPlace and runs within the WorkPlace window. Users must keep the WorkPlace window open while working with OnDemand in this embedded mode.

ⓘ | **NOTE:**

- Users cannot start an application from the OnDemand window. Unless you configure a URL to launch automatically when users start OnDemand, users must manually start applications as they would normally.

- Users may need to configure their personal firewalls to allow OnDemand traffic.

How OnDemand Redirects Network Traffic

OnDemand uses the local loopback address to redirect and secure traffic through the appliance. This section provides an overview of loopback proxying and describes the various redirection methods.

Topics:

- Overview: Loopback Proxying
- Hosts File Redirection

Overview: Loopback Proxying

OnDemand uses local loopback proxying to securely submit application traffic through the Web proxy service. For example, suppose a Windows user wants to connect to the appliance and run a Citrix application:

1. The user logs in to WorkPlace, and OnDemand automatically starts.
2. OnDemand dynamically maps the local loopback address to the host name for the Citrix server.
3. The user runs the Citrix application, which attempts to connect to *`citrix.example.com`*. OnDemand resolves the Citrix host name to `127.0.0.1` and routes the traffic to the Web proxy service.
4. OnDemand encrypts the Citrix traffic using SSL and securely routes it to the SMA appliance, which in turn forwards it to the Citrix server.
5. The Citrix server responds, sending data back through the SMA appliance.
6. The appliance forwards the response to OnDemand over SSL.
7. OnDemand forwards the information to the Citrix application.

Hosts File Redirection

To redirect traffic to destination servers, modify the hosts file on the user’s computer. This redirection method is supported on Windows, MacOS, and Linux platforms, provided the user has administrator privileges on the local computer.

Modifying the hosts file on a user’s system maps a destination server to a local loopback address. When an application attempts to resolve a host name, traffic is redirected to the loopback address on which OnDemand is listening.

The below table shows a typical hosts file, with host names mapped to IP addresses, followed by a hosts file modified for use by OnDemand.

Hosts Files

Typical Hosts File

	192.168.1.135 telnet.example.com telnet
	192.168.1.140 mailhost.example.com mail
	192.168.1.143 citrix.example.com citrix
OnDemand Hosts File	
	127.0.0.1 telnet.example.com telnet
	127.0.0.1 mailhost.example.com mail
	127.0.0.1 citrix.example.com citrix

> **NOTE:** The OnDemand host names are mapped to the local loopback address, not the host's IP address. For application-specific configurations, these loopback addresses would match the addresses you specify when configuring OnDemand in AMC; for more information, see Configuring OnDemand to Access Specific Applications.

Configuring OnDemand to Access Specific Applications

If you are deploying OnDemand to users on non-Windows platforms, or want to automatically use the launch URL feature to start a thin-client application when users run OnDemand, you must define an application-specific configuration in AMC. This involves mapping the port numbers for the client and server, a process called port mapping.

Topics:

- About Port Mapping
- Configuring an Application for Use with OnDemand

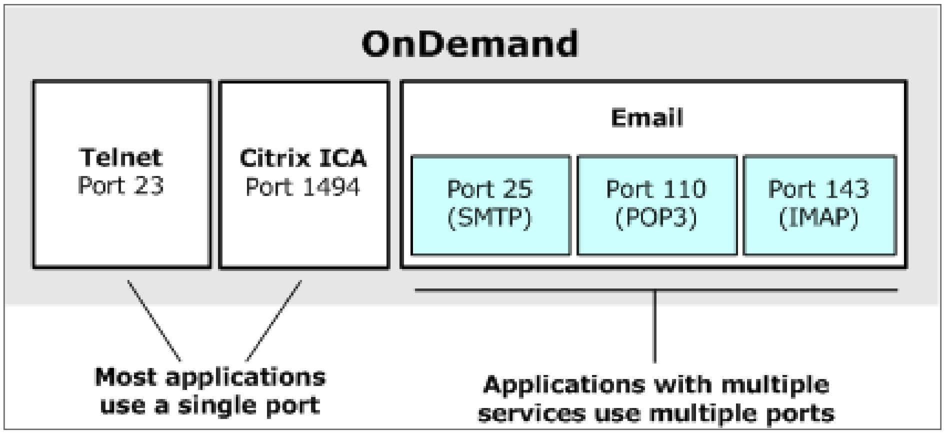
About Port Mapping

To configure OnDemand to redirect traffic for a specific application, you need to know the port numbers the application uses for the client and server, and then map those ports in AMC. OnDemand listens for incoming requests on specific ports on the client and then proxies them to the appliance, which forwards the information to an IP address and port on the application server.

For example, you might configure an IP address and port on the client (such as *127.0.1.1:23*) to the host or IP address and port on the destination server, such as *telneta.example.com:23*.

Some applications—such as email—use multiple ports for different protocols. In this case, you must configure OnDemand to listen on several different ports. This configuration can also be useful for configuring OnDemand to work with several different applications. The below image shows OnDemand configured to work with three applications over five different ports.

Example: OnDemand Configuration


OnDemand
Telnet
Port 23
Citrix ICA
Port 1494
Email
Port 25
(SMTP)
Port 110
(POP3)
Port 143
(IMAP)
Most applications use a single port
Applications with multiple services use multiple ports

In this example OnDemand is configured to listen on port 23 for telnet and port 1494 for Citrix. For email requests it is listening on port 25 (SMTP), port 110 (POP3), and port 143 (IMAP).

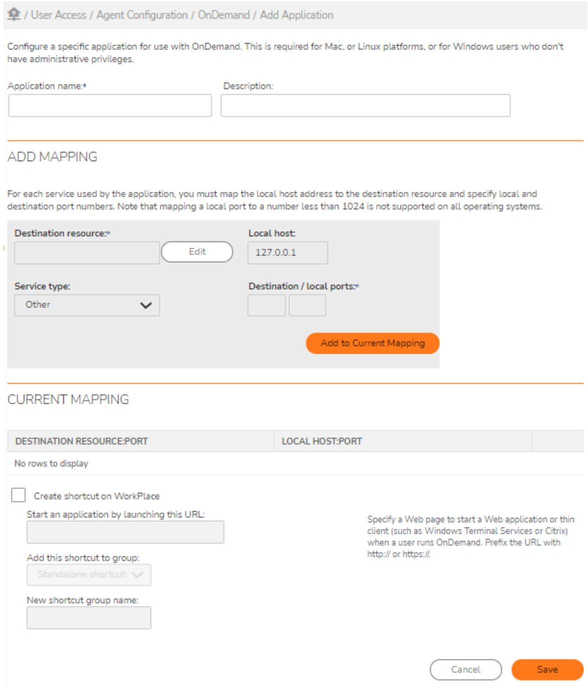
Configuring an Application for Use with OnDemand

To configure an application, you need to know the protocols it uses for each service and map the source address and ports on the client to those on the destination host. You also have the option of specifying a URL to open a Web page, which is useful for automatically starting an application, when the user runs OnDemand.

To configure an application for use with OnDemand:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. In the **Access Agents** section, click **Edit** next to **OnDemand**.

   The **Configure OnDemand** page displays.
3. In the **Mapped mode** area, click the **+** (New) icon.



/ User Access / Agent Configuration / OnDemand / Add Application

Configure a specific application for use with OnDemand. This is required for Mac, or Linux platforms, or for Windows users who don't have administrative privileges.

Application name:*

Description:

ADD MAPPING

For each service used by the application, you must map the local host address to the destination resource and specify local and destination port numbers. Note that mapping a local port to a number less than 1024 is not supported on all operating systems.

Destination resource:*

Local host: 127.0.0.1

Service type: Other

Destination / local ports:*

CURRENT MAPPING

DESTINATION RESOURCE:PORT	LOCAL HOST:PORT	
No rows to display		

□ Create shortcut on WorkPlace

Start an application by launching this URL:

Add this shortcut to group: Standalone shortcut:

New shortcut group name:

Specify a Web page to start a Web application or thin client (such as Windows Terminal Services or Citrix) when a user runs OnDemand. Prefix the URL with http:// or https://.

4. In the **Application name** field, type the name to use for the application. This name is displayed to the user in WorkPlace. Use a short, descriptive name.
5. In the **Description** field, type a descriptive comment about the application.
6. Configure each service used by the application in the **Add mapping** area.
    a. Click the **Edit** button beside the **Destination resource** field, select the network resource you want to configure, and then click **Save**. Alternatively, you can create a new network resource by clicking the **New Resource** button in the **Resources**.

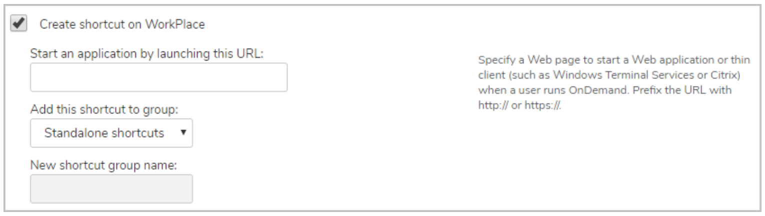
    b. If the IP address/port combination of the service conflicts with that of another service, you can modify the IP address displayed in the **Local host** field, or you can map the ports as described below. You can change the **Local host** value to any IP address in the `127.x.y.z` address space.

    ⓘ **NOTE:** On MacOS, OnDemand works only when using IP address `127.0.0.1` for the local host.

    c. In the **Service type** drop-down menu, select the type of service used by the application. This populates the **Destination/local ports** fields with the well-known port for that service. If the service uses a destination port that differs from that of the local port, map the ports to each other by editing the information in the **Destination/local ports** boxes as needed.

    d. Click **Add to Current Mapping**.

    This adds the mapping to the **Current mapping** list.
7. If the application uses multiple services, repeat *Step 6* to configure each one. Most applications use only one service, but some (like email) use multiple protocols, which requires multiple services.
8. Select the **Create shortcut on WorkPlace** checkbox.



☑ Create shortcut on WorkPlace

Start an application by launching this URL:

Add this shortcut to group: Standalone shortcuts

New shortcut group name:

Specify a Web page to start a Web application or thin client (such as Windows Terminal Services or Citrix) when a user runs OnDemand. Prefix the URL with http:// or https://.

- If you want OnDemand to open a Web page automatically (which is useful for automatically starting a thin-client application), type the URL of the appropriate page in the **Start an application by launching this URL** field. You must specify either an `http://` or an `https://`protocol identifier. The URL you specify automatically opens in a new browser window after OnDemand loads.
- In WorkPlace you can set up groups to organize resources for your users, or have shortcuts appear singly. In the **Add this shortcut to group** drop-down menu, select a new or existing group to which to add your shortcut, or select **Standalone shortcuts** if you want it to appear on its own. (The order in which shortcuts appear can be changed on the **Configure WorkPlace Layout** page; see Creating or Editing a WorkPlace Layout for more information.)

NOTE: After you initially configure the Create shortcut on WorkPlace option, you can view its setting only on the Mapped Mode page; you cannot edit it on this page. After initially configuring this setting, shortcuts are managed from the Shortcuts page in AMC. For more information, see Working with WorkPlace Shortcuts.

Client Configuration

This section explains client-side configuration that may be useful for working with OnDemand.

Topics:

- Configuring a Proxy Server in the Web Browser

Configuring a Proxy Server in the Web Browser

When passing an outbound connection over a proxy server, OnDemand uses the Web browser's settings to determine the proxy server address and port. This configuration requires the user to configure his or her Web browser, either by specifying the outbound proxy server address and port or by enabling automatic proxy detection.

If a user enables both automatic proxy detection and manual proxy identification, OnDemand checks for proxy server settings in this order:

1. If the **Automatically detect settings** option is enabled, OnDemand attempts to automatically detect the proxy server settings.
2. If OnDemand is unable to automatically detect the proxy server settings, it checks to see if the **Use automatic configuration script** option is enabled.
3. If OnDemand is unable to detect the proxy server settings through a configuration script, it uses the proxy server settings that the user manually specified.

To configure automatic proxy detection in browser for Windows:

1. On the **Tools** menu, click **Internet Options**.
2. On the **Connections** tab, click **LAN Settings**.
3. Under **Automatic Configuration**, enable one or both of the options:
   - To automatically detect proxy-server settings, select the **Automatically detect settings** checkbox. (This option is supported only for users running in any browser with the Microsoft Virtual Machine.)
   - To use configuration information contained in a configuration file, select the **Use automatic configuration script** checkbox and then, in the **Address** field, type the URL or path for the configuration file.

To manually specify proxy server settings in browser for Windows:

1. On the **Tools** menu, click **Internet Options**.
2. On the **Connections** tab, click **LAN Settings**.
3. Under **Proxy Server**, select the **Use a proxy server** checkbox, and specify the IP address and port for it.

   If a different proxy server is used for different protocols, click **Advanced** and specify the necessary information; be sure to specify proxy servers for both **HTTP** and **Secure**.

   > △ **CAUTION: Enabling either of the automatic settings in the LAN Settings (Automatically detect settings or Use automatic configuration script) may override the proxy server settings; clear these two checkboxes to ensure that proxy detection works correctly.**

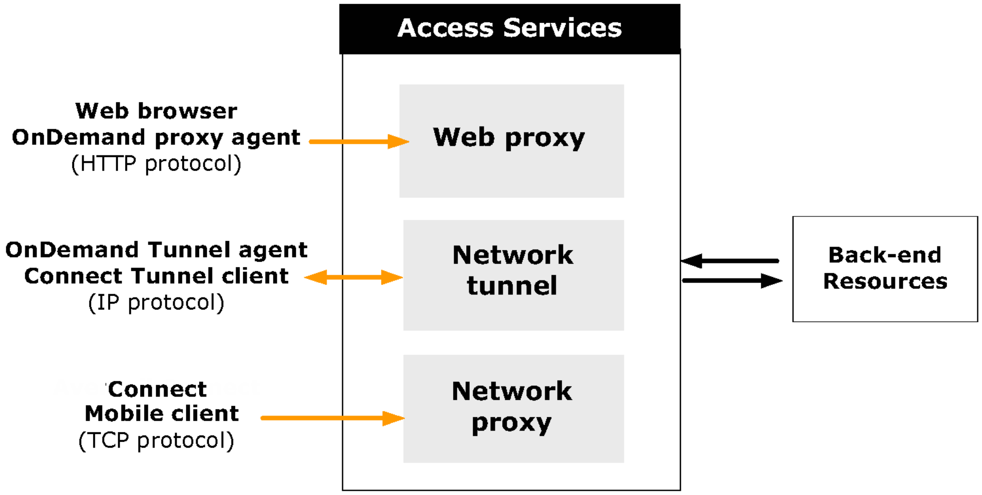
Managing Access Services

This section provides an overview of the access services, and describes how to start, stop, and configure the services.

Topics:

- About Access Services
- Stopping and Starting the Secure Mobile Access Services
- Configuring the Network Tunnel Service
- Configuring IP Address Pools
- Configuring Web Resource Filtering
- Device VPN endpoint enrollment
- Configuring Custom Connections
- Configuring the Web Proxy Service

About Access Services



Users can access VPN resources secured by the SMA appliance using three primary methods, or access services. This section describes each of the access services and the types of resources they provide access to.

- **The network tunnel service** is a network routing technology that provides secure network tunnel access to a wide range of client/server applications, including those that use non-TCP protocols such as VoIP and ICMP, reverse-connection protocols, and bi-directional protocols, such as those used by remote Help Desk applications. It works in conjunction with the Connect Tunnel client and the OnDemand Tunnel agent to provide authenticated and encrypted access. The network tunnel service can traverse firewalls, NAT devices, and other proxy servers that can interfere with traditional VPN devices.

  When Web resource filtering is enabled for the network tunnel service, policies for tunnel sessions can use URL-based rules in addition to IP-based rules.

- **The WorkPlace service** controls access to network file shares accessed from a Web browser. The WorkPlace service communicates with Windows file servers and network shares (including Microsoft Distributed file system, or Dfs, resources) using the Server Message Block (SMB) file-sharing protocol. For information about configuring the WorkPlace service, see Configuring WorkPlace General Settings.

The below table illustrates the relationships between the Secure Mobile Access access services and the user access components that they control.

Relationships Between SMA Access Services And User Access Components

Service	User access components	Description

Network tunnel service	• OnDemand Tunnel agent • Connect Tunnel client	• Manages TCP/IP and non-TCP (such as VoIP and ICMP) connections from the network tunnel clients. • Provides network-level access to all resources, effectively making the user's computer a node on your network. • Includes support for mapped network drives, native email clients, and applications that make reverse connections, such as VoIP.
Web proxy service	• Translated Web access • Custom port mapped Web access • Custom FQDN mapped Web access	• Manages HTTP and TCP/IP connections from Web browsers.
WorkPlace service	• WorkPlace portal	• Provides a Web-based portal that is available from any Web browser. • Provides access to file-system resources. • Provisions and deploys all user access components.

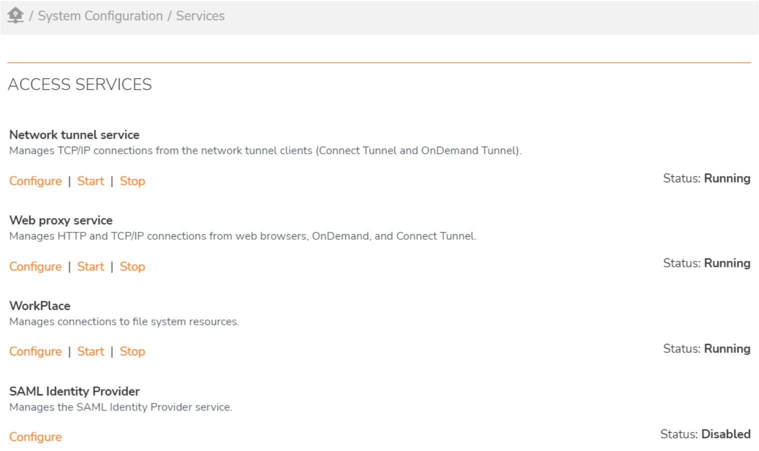
Stopping and Starting the Secure Mobile Access Services

You may occasionally want to temporarily stop one of the Secure Mobile Access services.

△ **CAUTION: SonicWall recommends stopping the services only during scheduled maintenance periods or during off hours. Also, you should give your users advance warning that the service will be going down.**

To start or stop a service:

1. In the AMC, navigate to **System Configuration > Services**.



/ System Configuration / Services

ACCESS SERVICES

Network tunnel service
Manages TCP/IP connections from the network tunnel clients (Connect Tunnel and OnDemand Tunnel).
Configure | Start | Stop — Status: **Running**

Web proxy service
Manages HTTP and TCP/IP connections from web browsers, OnDemand, and Connect Tunnel.
Configure | Start | Stop — Status: **Running**

WorkPlace
Manages connections to file system resources.
Configure | Start | Stop — Status: **Running**

SAML Identity Provider
Manages the SAML Identity Provider service.
Configure — Status: **Disabled**

2. Under **Access Services**, click the appropriate link:
   - Click **Stop** to stop the service. All existing user connections will be terminated.
   - Click **Start** to start the service.

Configuring the Network Tunnel Service

The network tunnel service controls access from the Connect Tunnel client, the OnDemand Tunnel agent, and the Mobile Connect agent. In order to deploy the network tunnel clients to users, you must first make one or more IP address pools available to the community. Configuring the network tunnel service requires setting up IP address pools that are used to allocate IP addresses to the clients; these IP addresses become the clients' end points on VPN connections.

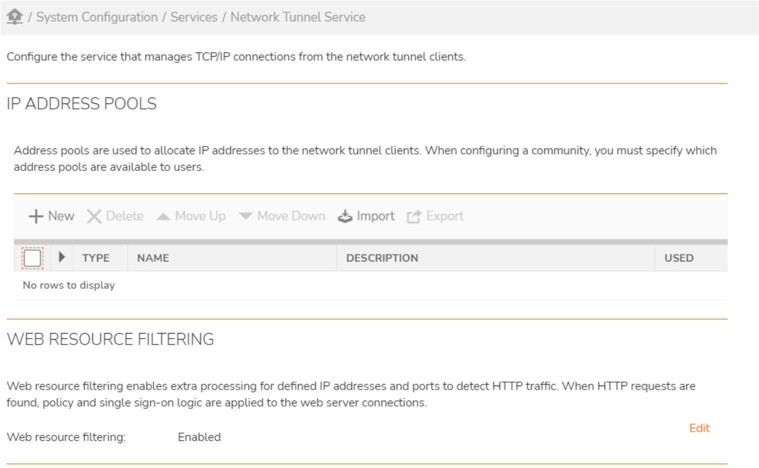
Network tunnel service configuration also allows you to enable Web resource filtering so that you can enforce the same URL-based rules that administrators define for Workplace in tunnel sessions. Web resource filtering also allows you to leverage single sign-on functionality when accessing Web applications.

You can add custom connections to configure Connect Tunnel to access a different default appliance or realm, or list other appliances and realms the client can connect to. By default, Connect Tunnel is configured to access the realm and appliance from which it was downloaded.

To configure the network tunnel service:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, **Configure**.

   The **Network Tunnel Service** page displays.



Configure the service that manages TCP/IP connections from the network tunnel clients.

IP ADDRESS POOLS

Address pools are used to allocate IP addresses to the network tunnel clients. When configuring a community, you must specify which address pools are available to users.

□	TYPE	NAME	DESCRIPTION	USED
No rows to display				

WEB RESOURCE FILTERING

Web resource filtering enables extra processing for defined IP addresses and ports to detect HTTP traffic. When HTTP requests are found, policy and single sign-on logic are applied to the web server connections.

Web resource filtering: Enabled

3. In the **IP Address Pools** area, create one or more IP address pools. For more information, see Configuring IP Address Pools.
4. To enable and configure Web resource filtering, click **Edit** in the **Web resource filtering** area. For more information, see Configuring Web Resource Filtering.
5. To configure a custom connection in which Connect Tunnel can access the current or a different default appliance or realm, or list other appliances and realms the client can connect to, click the **New** button in the **Custom Connections** area. For more information, see Configuring Custom Connections.

Configuring IP Address Pools

IP address pools are used to allocate IP addresses to the network tunnel clients. When a user makes a connection using the Connect Tunnel client, the OnDemand Tunnel agent, or the Mobile Connect agent, the SMA appliance assigns the client an IP address from one of its configured address pools. Only pools allowed for the client's community are considered. For more information about how IP addresses are allocated to a community, see IP Address Allocation.

For information about editing and deleting IP address pools, see Adding, Editing, Copying, and Deleting Objects in AMC.

Topics:

- Address Pool Allocation Methods
- Best Practices for Configuring IP Address Pools
- Adding Translated IP Address Pools
- Adding Dynamic IP Address Pools
- Adding a Dynamic, RADIUS-Assigned IP Address Pools
- Adding Static IP Address Pools

Address Pool Allocation Methods

You can configure IP address allocation in the following ways:

- Translated Address Pools (Source NAT)
- Routed Address Pools (DHCP)
- RADIUS-Assigned Address Pools
- Static Address Pools

Translated Address Pools (Source NAT)

With translated address pools, the appliance assigns non-routable IP addresses to clients and uses source network address translation (Source NAT) to translate them to a single address you configure for back-end traffic. The appliance uses the name servers you specify in AMC to define the DNS and WINS settings on the client. Source NAT translates the client's non-routable source address to a single configured address from a fixed, non-routable sequence (`2.0.0.2` through `2.255.254.254`) on the internal network.

ⓘ **NOTE:** Translated address pools is ideally intended for SMA deployments of less than 250 concurrent users. Using translated address pools in deployments with more than that number of concurrent users can lead to issues with connectivity and system stability.

The advantages of using translated address pools are:

- Source NAT address pools require only a single back-end address, which is shared by all remote connections.
- Fewer IP addresses are required for the tunnel clients.

The constraints of this type of pool are:

- All network activity must be initiated by the client; therefore, this method of IP address allocation does not support applications that make reverse connections or cross-connections (such as SMS, VoIP, or FTP).
- Windows domain browsing is not supported; if users try to browse a Windows domain through Network Explorer or Network Neighborhood, an error message indicates that they are not authorized to access the resources.
- Client-to-client cross-connections are not supported.

Routed Address Pools (DHCP)

With a routed address pool, IP addresses are dynamically allocated to the tunnel clients from a DHCP server. DHCP address pools have these characteristics:

- They require an external server that has enough spare addressing capacity to support the new remote clients. These pools are easy to set up and maintain, and impose few restrictions on client activity.
- Reverse connections and cross-connections are supported, but client IP addresses must be known. If necessary, you can associate a fixed DHCP address with a particular client by configuring the DHCP client ID on the DHCP server. Client IDs are generated during client configuration; consult the DHCP server logs to find particular IDs.

RADIUS-Assigned Address Pools

Some applications require a one-to-one relationship between an assigned IP address and a user. This is best supported by a RADIUS server, where IP address allocation happens during the authorization process, as part of authentication.

This strict one-to-one correlation may have some unintended consequences:

- For example, if an employee is logged in to the appliance at work and forgets to log out, logging in from home will fail: the IP address is still attached to the original tunnel connection at the office. Optionally, you can configure the community and realm in AMC that is referencing the RADIUS server to use other IP address pools if the RADIUS pool is exhausted.
- If you have two appliances authenticating against the same RADIUS server and both are using RADIUS pools, duplicate address assignments will be made, resulting in multiple network conflicts.

Static Address Pools

With static address pools, you specify one or more static IP address pools from which IP addresses will be allocated to the tunnel clients. You can configure static IP address pools as subnets or address ranges. Static address pools have these characteristics:

- Static address pools require no configuration work outside of the appliance, and they support reverse connections and cross-connections.
- Static pools require identification of one back-end address per simultaneous remote connection. If enough addresses are available to cover all possible remote clients (not just simultaneous connections) and no address conflicts occur, this method tends to be the most stable because the same address is typically assigned to the same client.
- Static pools leave an IP address assigned as long as the tunnel remains up. If the tunnel goes down, there is a two-minute period during which the address is available, but only for reassignment to the same client. After that two minute period expires, the address is available to any client; address reassignment is performed using an LRU (Least Recently Used) scheme.
- Windows domain browsing is supported.

Best Practices for Configuring IP Address Pools

Here are some best practices to keep in mind when configuring IP address pools:

- Don’t duplicate addresses:
  - When configuring static IP address pools, do not specify IP addresses that are already assigned to other network resources.
  - Be aware that any IP addresses you configure for use by the network tunnel clients may conflict with IP addresses already in use on the client networks. Whenever possible, avoid configuring IP addresses that you know to be in use on your users’ networks.

  - When configuring translated (Source NAT) IP address pools, be sure to specify an unused address on the subnet of the internal interface.
  - If you are using RADIUS pools on more than one appliance, and the appliances are authenticating against the same RADIUS server, duplicate address assignments will be made.
- When configuring dynamic DHCP or static IP address pools, ensure that you have enough IP addresses to accommodate your maximum number of concurrent users. For example, if your maximum concurrent user count is 100, you should make at least 100 IP addresses available.

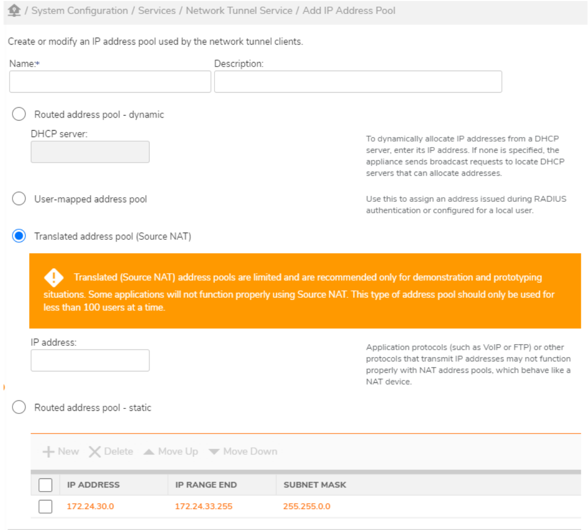
Adding Translated IP Address Pools

This section describes how to create a translated IP address pool using secure network address translation (Source NAT).

> ⓘ **NOTE:** Translated (Source NAT) address pools are limited and are recommended only for demonstration and prototyping situations. Some applications will not function properly using Source NAT. This type of address pool should only be used for less than 100 users at a time.

To add a translated IP address pool:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, Configure. The **Network Tunnel Service** page displays.
3. In the **IP Address Pools** area, click the **+** (New) icon. The **IP Address Pool** page displays.



/ System Configuration / Services / Network Tunnel Service / Add IP Address Pool

Create or modify an IP address pool used by the network tunnel clients.

Name:*

Description:

○ Routed address pool - dynamic

DHCP server:

To dynamically allocate IP addresses from a DHCP server, enter its IP address. If none is specified, the appliance sends broadcast requests to locate DHCP servers that can allocate addresses.

○ User-mapped address pool

Use this to assign an address issued during RADIUS authentication or configured for a local user.

● Translated address pool (Source NAT)

Translated (Source NAT) address pools are limited and are recommended only for demonstration and prototyping situations. Some applications will not function properly using Source NAT. This type of address pool should only be used for less than 100 users at a time.

IP address:

Application protocols (such as VoIP or FTP) or other protocols that transmit IP addresses may not function properly with NAT address pools, which behave like a NAT device.

○ Routed address pool - static

□	IP ADDRESS	IP RANGE END	SUBNET MASK
□	172.24.30.0	172.24.33.255	255.255.0.0

4. In the **Name** field, type a name for the address pool.
5. In the **Description** field, type a descriptive comment about the address pool.
6. Click **Translated address pool (Source NAT)**.
7. In the **IP address** field, type the Source NAT address that will appear to back-end servers as the source of

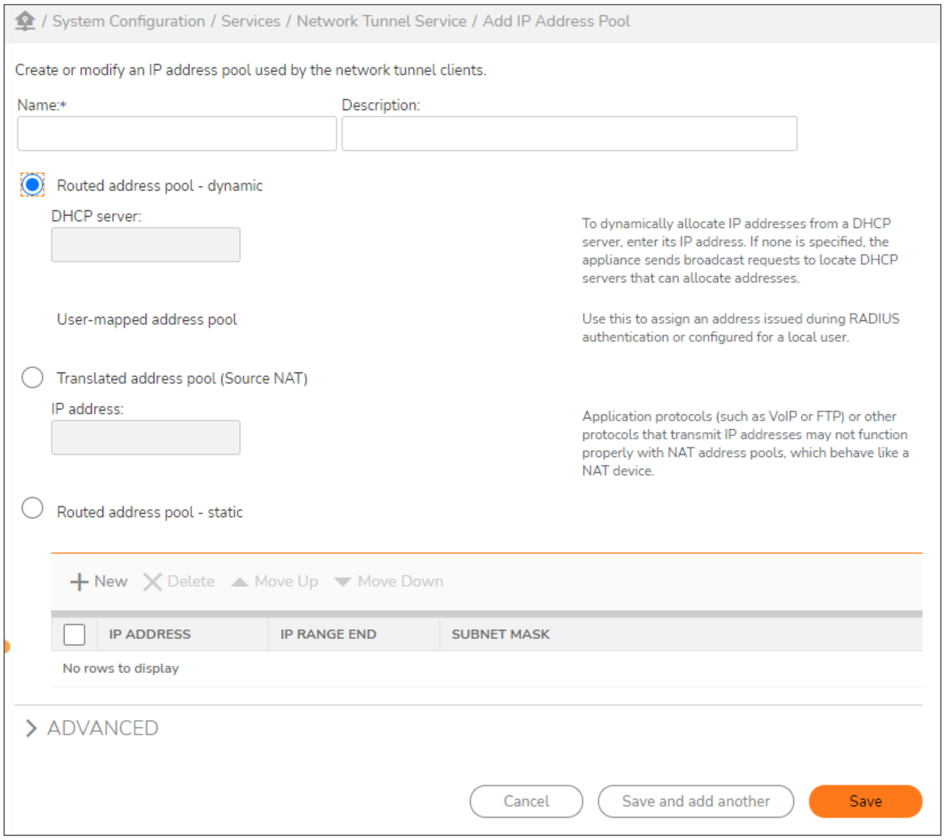
all client traffic. Ensure that this IP address is not in use elsewhere.

8. Click **Save**.

Adding Dynamic IP Address Pools

To add a dynamic IP address pool:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, **Configure**. The **Network Tunnel Service** page displays.
3. In the **IP Address Pools** section, click the **+** (New) icon. The **IP Address Pool** page displays.



/ System Configuration / Services / Network Tunnel Service / Add IP Address Pool

Create or modify an IP address pool used by the network tunnel clients.

Name:*

Description:

● Routed address pool - dynamic

DHCP server:

To dynamically allocate IP addresses from a DHCP server, enter its IP address. If none is specified, the appliance sends broadcast requests to locate DHCP servers that can allocate addresses.

User-mapped address pool

Use this to assign an address issued during RADIUS authentication or configured for a local user.

○ Translated address pool (Source NAT)

IP address:

Application protocols (such as VoIP or FTP) or other protocols that transmit IP addresses may not function properly with NAT address pools, which behave like a NAT device.

○ Routed address pool - static

□	IP ADDRESS	IP RANGE END	SUBNET MASK

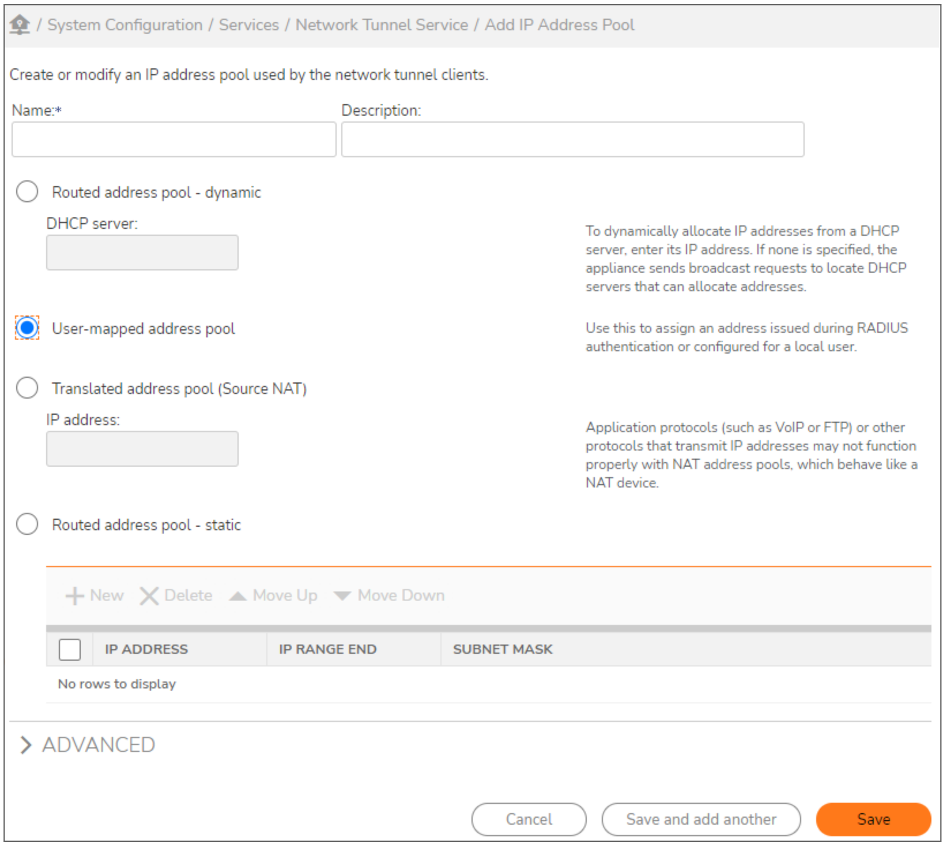
No rows to display

4. In the **Name** field, type a name for the address pool.
5. In the **Description** field, type a descriptive comment about the address pool.
6. Click **Routed address pool - dynamic**.
7. By default the **DHCP server** field is blank; the appliance sends broadcast requests to locate DHCP servers and uses them to allocate addresses. Leave this box blank unless you need to configure a specific DHCP server.
8. Click **Save.** (DHCP address pools ignore the **Advanced** settings on this AMC page.)

Adding a Dynamic, RADIUS-Assigned IP Address Pools

To add a RADIUS-assigned IP address pool:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, **Configure**. The **Network Tunnel Service** page displays.
3. In the **IP Address Pools** section, click the **+** (New) icon. The **IP Address Pool** page displays.



/ System Configuration / Services / Network Tunnel Service / Add IP Address Pool

Create or modify an IP address pool used by the network tunnel clients.

Name:* Description:

○ Routed address pool - dynamic

DHCP server:

To dynamically allocate IP addresses from a DHCP server, enter its IP address. If none is specified, the appliance sends broadcast requests to locate DHCP servers that can allocate addresses.

● User-mapped address pool

Use this to assign an address issued during RADIUS authentication or configured for a local user.

○ Translated address pool (Source NAT)

IP address:

Application protocols (such as VoIP or FTP) or other protocols that transmit IP addresses may not function properly with NAT address pools, which behave like a NAT device.

○ Routed address pool - static

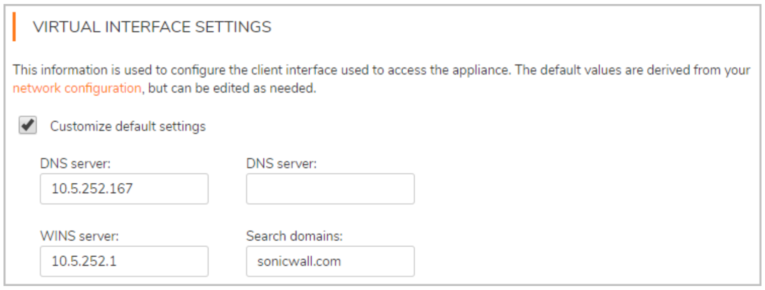
+ New ✕ Delete ▲ Move Up ▼ Move Down

□	IP ADDRESS	IP RANGE END	SUBNET MASK

No rows to display

> ADVANCED

4. In the **Name** field, type a name for the address pool.
5. In the **Description** field, type a descriptive comment about the address pool.
6. Click **User-mapped address pool** to configure a pool in which IP address allocation is made during the authorization process, as part of authentication. You would choose this setting if, for example, you have an application that requires a one-to-one relationship between an assigned IP address and a user.
7. (Optional) To change the virtual interface settings for configuring the client interface, click to expand the **Advanced** area. The **Virtual interface settings** are preconfigured with the **DNS server**, **WINS server**, and **Search domains** as defined on the **Network Settings** page. (For more information, see Configuring Basic Network Settings.) To change these settings, select the **Customize default settings** checkbox and then specify custom values for any settings that you want to change.



VIRTUAL INTERFACE SETTINGS

This information is used to configure the client interface used to access the appliance. The default values are derived from your network configuration, but can be edited as needed.

☑ Customize default settings

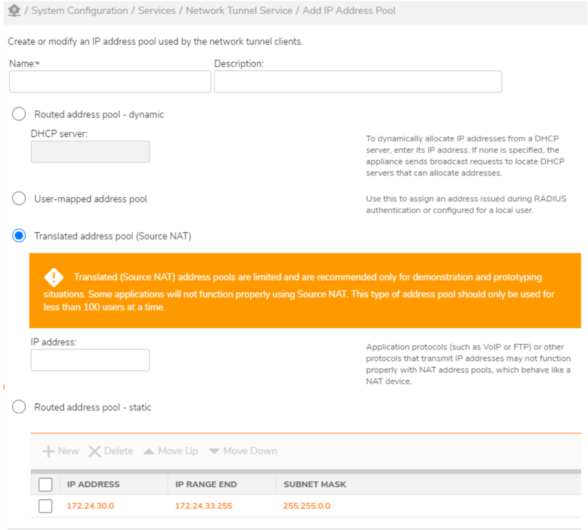
DNS server: 10.5.252.167	DNS server:
WINS server: 10.5.252.1	Search domains: sonicwall.com

8. Click **Save**.

Adding Static IP Address Pools

To add a static IP address pool:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, **Configure**. The **Network Tunnel Service** page displays.
3. In the **IP Address Pools** section, click the **+** (New) icon. The **IP Address Pool** page displays.



/ System Configuration / Services / Network Tunnel Service / Add IP Address Pool

Create or modify an IP address pool used by the network tunnel clients.

Name:*	Description:

○ Routed address pool - dynamic

DHCP server:

To dynamically allocate IP addresses from a DHCP server, enter its IP address. If none is specified, the appliance sends broadcast requests to locate DHCP servers that can allocate addresses.

○ User-mapped address pool

Use this to assign an address issued during RADIUS authentication or configured for a local user.

● Translated address pool (Source NAT)

Translated (Source NAT) address pools are limited and are recommended only for demonstration and prototyping situations. Some applications will not function properly using Source NAT. This type of address pool should only be used for less than 100 users at a time.

IP address:

Application protocols (such as VoIP or FTP) or other protocols that transmit IP addresses may not function properly with NAT address pools, which behave like a NAT device.

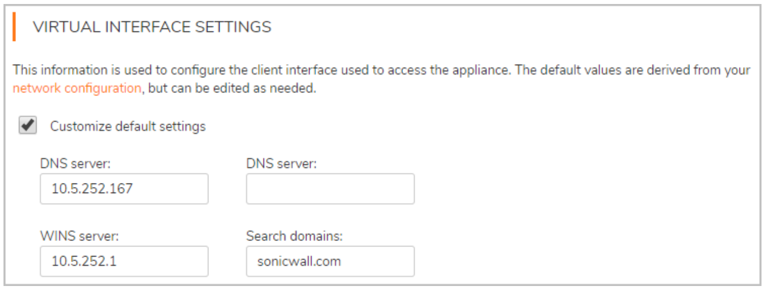
○ Routed address pool - static

□	IP ADDRESS	IP RANGE END	SUBNET MASK
□	172.24.30.0	172.24.33.255	255.255.0.0

4. In the **Name** field, type a name for the address pool.
5. In the **Description** field, type a descriptive comment about the address pool.
6. Click **Routed address pool - static**, and then click **New**.
7. Specify the IP address or addresses to make available to the tunnel clients. Type IP addresses and subnet masks using dotted decimal form (`n.n.n.n`).
   - To define a single host, type an **IP address** and a **Subnet mask** of `255.255.255.255`.
   - To specify a range of IP addresses, type the beginning address in the IP address field and the ending address in the **IP range end** field, and specify a **Subnet mask**.

- To define an entire subnet, type the network address in the **IP address** field and fill in the **Subnet mask** field. The subnet mask is converted to a range and values are filled in as appropriate. If the IP address of the subnet is entered, it is converted to the first usable address in the network, but addresses in the middle of the subnet are used as is. The ending address is filled in with the highest usable address in the subnet.

8. Click **OK**. The pool is added to the list of available IP address pools.
9. (Optional) To change the virtual interface settings for configuring the client interface, click to expand the **Advanced** area. The **Virtual interface settings** are preconfigured with the **DNS server**, **WINS server**, and **Search domains** as defined on the **Network Settings** page. (For more information, see Configuring Basic Network Settings.) To change these settings, select the **Customize default settings** checkbox and then specify custom values for any settings that you want to change.



VIRTUAL INTERFACE SETTINGS

This information is used to configure the client interface used to access the appliance. The default values are derived from your network configuration, but can be edited as needed.

☑ Customize default settings

DNS server: 10.5.252.167

DNS server:

WINS server: 10.5.252.1

Search domains: sonicwall.com

10. Click **Save**.

Configuring Web Resource Filtering

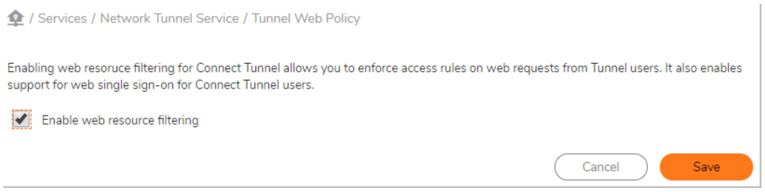
Web resource filtering enables extra processing for defined IP addresses and ports to detect HTTP traffic. When HTTP requests are found, policy and single sign-on logic are applied to the Web server connections.

Web resource filtering allows you to enforce the same URL-based rules in tunnel sessions that administrators define for Workplace. It also allows you to leverage single sign-on functionality when accessing Web applications.

When Web resource filtering is not enabled, the available policies for Web access and tunnel access are not equivalent. The Web access cases can evaluate URL policy for all translated access and HTTP access for Web proxy and port map clients. For users connected via a tunnel, the IP layer redirection only permits policies based on IP address. In deployments where multiple Web addresses or namespaces are hosted on a single Web server, all Web content is reachable at a single IP address or pool of addresses. Basing policy on just the IP layer does not permit the administrator to enforce policy distinctions between the multiple namespaces. Enabling Web resource filtering allows policies to use URL-based rules in addition to IP-based rules for tunnel sessions.

To configure Web resource filtering:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, **Configure**. The **Network Tunnel Service** page displays.
3. In the **Web Resource Filtering** section, click **Edit**. The **Tunnel Web Policy page** displays.


/ Services / Network Tunnel Service / Tunnel Web Policy

Enabling web resoruce filtering for Connect Tunnel allows you to enforce access rules on web requests from Tunnel users. It also enables support for web single sign-on for Connect Tunnel users.

☑ Enable web resource filtering

4. Select the **Enable web resource filtering** checkbox to cause the tunnel service to check all client traffic at ports that may contain Web network traffic.
5. Click **Save**.

Secure Network Detection

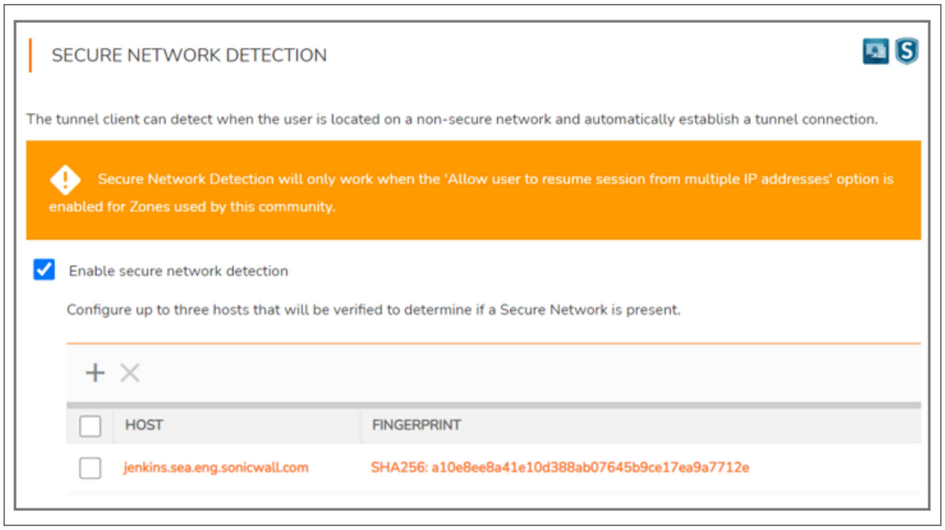
Secure Network Detection allows users to automatically establish a tunnel connection when attempting to login from an unsecure location. The client determines whether the device is in a secure network by validating the TLS connection to the configured secure host. When Secure Network Detection is enabled, the Connect Tunnel client can detect when the user is located on a non-secure network and automatically establish a tunnel connection.

ⓘ | **NOTE:** Mobile connect still follows DNS suffix entry for detecting secure network.

Secure Hosts for secure network detection can now be configured under community level and you can configure up to three secure hosts.

To configure secure host:

1. Log in to AMC.
2. Navigate to **User Access > Realms**.
3. Select the realm for which you want to configure the tunnel client.
4. Navigate to **Tunnel Access** tab and select **Enable secure network detection** checkbox.
5. Click + icon to add the secure host.
6. In the **Host** field, enter the host name or IP address which you want to verify for identifying secure network.
7. In the **Fingerprint** drop-down, select the secure hash algorithm based on your requirement. The supported algorithms are SHA256, and SHA1.



SECURE NETWORK DETECTION

The tunnel client can detect when the user is located on a non-secure network and automatically establish a tunnel connection.

Secure Network Detection will only work when the 'Allow user to resume session from multiple IP addresses' option is enabled for Zones used by this community.

☑ Enable secure network detection

Configure up to three hosts that will be verified to determine if a Secure Network is present.

□	HOST	FINGERPRINT
□	jenkins.sea.eng.sonicwall.com	SHA256: a10e8ee8a41e10d388ab07645b9ce17ea9a7712e

8. Click **Save**.

ⓘ | **NOTE:** You can configure up to three secure hosts.

Device VPN

Device VPN provides VPN access to a device on boot. VPN access is expected to be always available and limited to critical common resources that provide basic network access, logon, remote management, and remediation services (for devices lacking capability). For example, DNS, PDC, Windows Update and other critical services. The Device VPN session is non-interactive and establishes VPN connection in background.

Topic:

- Device VPN endpoint enrollment

ⓘ | **NOTE:** The device VPN endpoint enrollment is supported only for Windows based managed devices.

Device VPN endpoint enrollment

The device VPN feature depends on the client certificate to authenticate endpoint or a device for device-level VPN access.

Unless the customer has an existing Certificate Enrollment Web Service (CES) or Certificate Enrollment Policy (CEP) web service setup, deployment of device certificates is complex and becomes a hurdle for using Device VPN.

From 12.4.2. onwards, you can:

- Deploy client certificates on end devices for Device Tunnel authentication.
- Get details of the list of enrolled device certificates such as device certificate subject DN, Device ID, expiration date, and so on.
- Revoke or delete enrolled device certificates.

ⓘ | **NOTE:**

- An enrolled device certificate expires in 90 days and is auto-renewed 15 days prior to the expiry.

Topics:

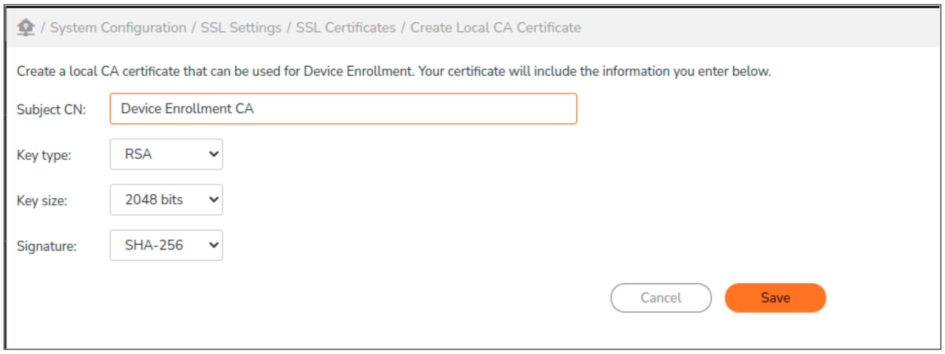
- Configuring Local CA in AMC
- Configuring a PKI Authentication Server
- Creating Device VPN Realms
- Configuring Device VPN
- Viewing and Deleting or Revoking Device VPN certificate

Refer to Establishing a Device VPN connection section *Connect Tunnel* guide to deploy client certificates on end devices for Device Tunnel authentication.

Configuring Local CA in AMC

To configure local CA:

1. In the AMC, navigate to **System Configuration** > **SSL Settings**.
2. In the **CA Certificates** section, click the + (New) icon.
3. Select **Local CA** to create local CA Certificate.



/ System Configuration / SSL Settings / SSL Certificates / Create Local CA Certificate

Create a local CA certificate that can be used for Device Enrollment. Your certificate will include the information you enter below.

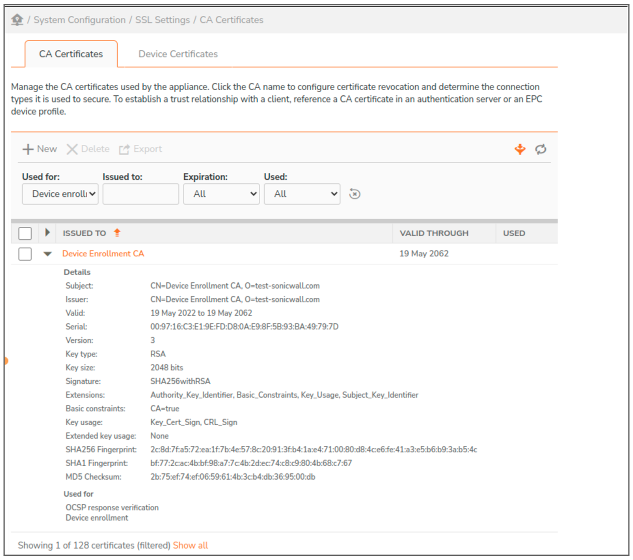
Subject CN: Device Enrollment CA

Key type: RSA

Key size: 2048 bits

Signature: SHA-256

4. In **SubjectCN** enter the CA value.
5. In the **Key type** drop-down, select the key type based on your requirement. The supported key types are **RSA** and **EC**.
6. In the **Key size** drop-down, select the key size based on your requirement. The supported key sizes are **2048**, **3072**, and **4096** bits.
7. In the **Signature** drop-down, select the Secure Hash algorithm based on your requirement. The supported signatures are SHA 512, SHA-384, and SHA-256.
8. Click **Save**.



Manage the CA certificates used by the appliance. Click the CA name to configure certificate revocation and determine the connection types it is used to secure. To establish a trust relationship with a client, reference a CA certificate in an authentication server or an EPC device profile.

Used for: Device enrollı
Issued to:
Expiration: All
Used: All

□	ISSUED TO	VALID THROUGH	USED
□	Device Enrollment CA	19 May 2062	

Details

Subject:	CN=Device Enrollment CA, O=test-sonicwall.com
Issuer:	CN=Device Enrollment CA, O=test-sonicwall.com
Valid:	19 May 2022 to 19 May 2062
Serial:	00:97:16:C3:E1:9E:FD:D8:0A:E9:8F:5B:93:BA:49:79:7D
Version:	3
Key type:	RSA
Key size:	2048 bits
Signature:	SHA256withRSA
Extensions:	Authority_Key_Identifier, Basic_Constraints, Key_Usage, Subject_Key_Identifier
Basic constraints:	CA=true
Key usage:	Key_Cert_Sign, CRL_Sign
Extended key usage:	None
SHA256 Fingerprint:	2c:8d:7f:a5:72:ea:1f:7b:4e:57:8c:20:91:3f:b4:1a:e4:71:00:80:d8:4c:e6:fe:41:a3:e5:b6:b9:3a:b5:4c
SHA1 Fingerprint:	bf:77:2c:ac:4b:bf:98:a7:7c:4b:2d:ec:74:c8:c9:80:4b:68:c7:67
MD5 Checksum:	2b:75:ef:74:ef:06:59:61:4b:3c:b4:db:36:95:00:db

Used for

OCSP response verification
Device enrollment

Showing 1 of 128 certificates (filtered) Show all

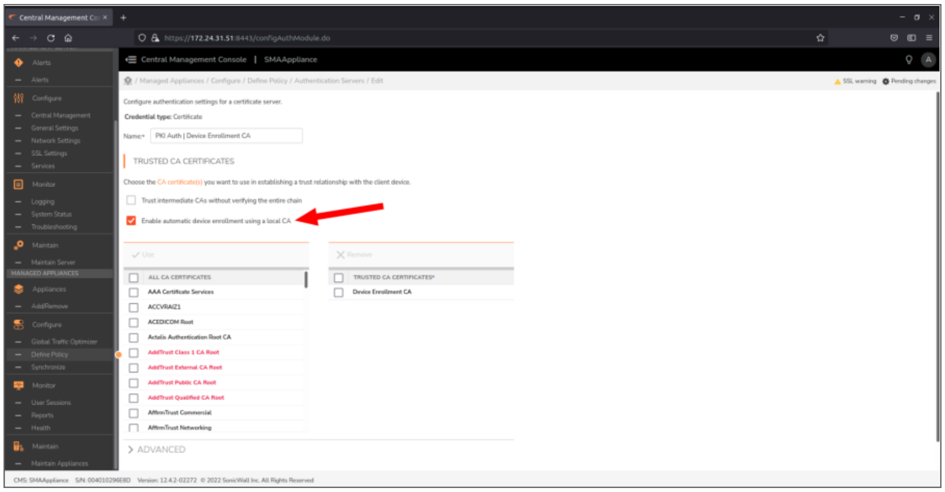
Refer to the Configuring Device VPN section for more details of the list of enrolled device certificates.

Configuring a PKI Authentication Server for Local CA

1. In the AMC, navigate to **System Configuration** > **Authentication Servers**.
2. Click **New**.
3. Under **Authentication directory** , click **Public key infrastructure** (PKI).
4. Click **Continue**.

   The **Edit Authentication Server** page displays.
5. In the **Name** field, type a name for the authentication server.
6. On the **Use** list, **All CA certificates** used by the appliance select local CA certificate.
7. Under **Trusted CA certificates**, select the **Enable automatic device enrollment using a local CA** checkbox.

   ⓘ **NOTE:** The **Enable automatic device enrollment using a local CA** checkbox is enabled only for PKI with local CA and not for any other CA.


Central Management Console | SMAAppliance
/ Managed Appliances / Configure / Define Policy / Authentication Servers / Edit
Alerts
Configure
Monitor
Maintain
MANAGED APPLIANCES
Appliances
Use
Remove
SSL warning
Pending changes

Configure authentication settings for a certificate server.

Credential type: Certificate

Name:* PKI Auth | Device Enrollment CA

TRUSTED CA CERTIFICATES

Choose the CA certificate(s) you want to use in establishing a trust relationship with the client device.

□ Trust intermediate CAs without verifying the entire chain

☑ Enable automatic device enrollment using a local CA

□	ALL CA CERTIFICATES
□	AAA Certificate Services
□	ACCVRAIZ1
□	ACEDICOM Root
□	Actalis Authentication Root CA
□	AddTrust Class 1 CA Root
□	AddTrust External CA Root
□	AddTrust Public CA Root
□	AddTrust Qualified CA Root
□	AffirmTrust Commercial
□	AffirmTrust Networking

□	TRUSTED CA CERTIFICATES*
□	Device Enrollment CA

> ADVANCED

CMS: SMAAppliance S/N: 004010296EBD Version: 12.4.2-02272 © 2022 SonicWall Inc. All Rights Reserved

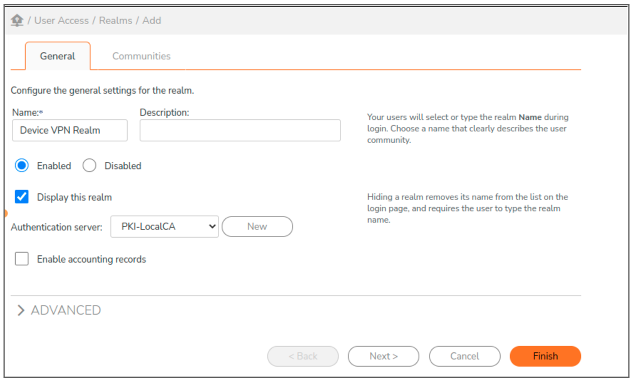
8. Configure other details and click **Save**.

Creating Device VPN Realms

1. In the AMC, navigate to **User Access** > **Realms**.
2. Click **+ New** realm.

   The **Configure Realm** page displays with the **General** settings for the realms.
3. In the **Name** field, enter the name for Auth server. For example, enter `Device VPN Realm`.
4. In the **Description** field, type a descriptive comment about the realm.
5. Enable or disable this realm by selecting the appropriate **Status**.
6. If you want this realm to appear in the list seen by your users (recommended in most cases), select the **Display this realm** checkbox.
7. From the **Authentication server** drop-down menu, select the configured Authentication Server.

   If you have created a Local CA for Device VPN enrollment, then select the Local CA PKI authentication server.



Configure the general settings for the realm.

Name:* Device VPN Realm

Description:

Your users will select or type the realm **Name** during login. Choose a name that clearly describes the user community.

● Enabled ○ Disabled

☑ Display this realm

Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

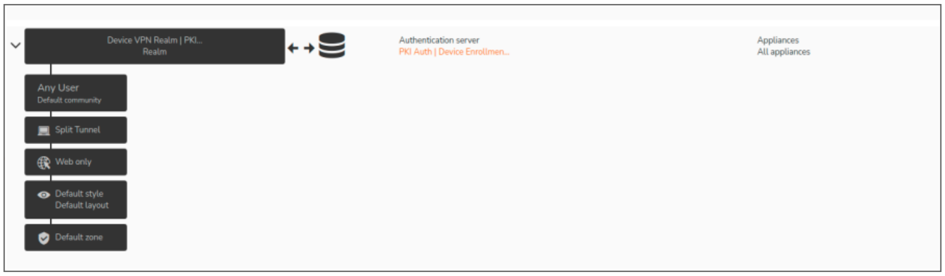
Authentication server: PKI-LocalCA

□ Enable accounting records

> ADVANCED

8. Click **Advanced** and configure the settings.

9. Click **Save**.



Authentication server: PKI Auth | Device Enrollmen...

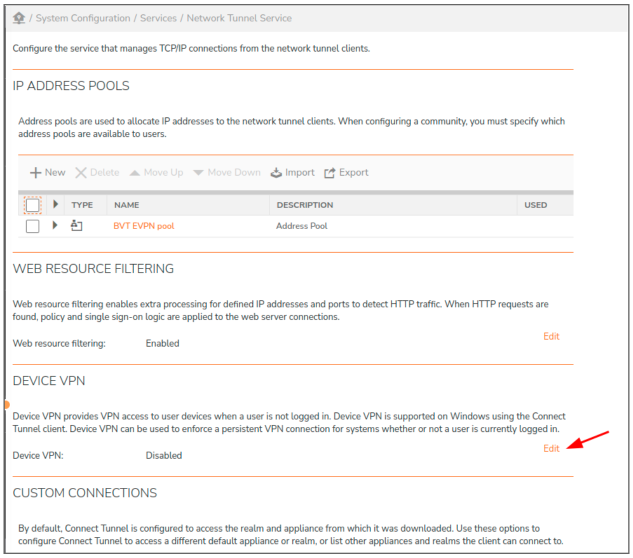
Appliances: All appliances

Configuring Device VPN

To configure Device VPN:

1. In the AMC, navigate to **System Configuration** > **Services**.
2. In the **Access Services** section, under **Network tunnel service** area, click **Configure**.

   The Network Tunnel Service page displays.
3. In the **Device VPN** section, click the **Edit**.



/ System Configuration / Services / Network Tunnel Service

Configure the service that manages TCP/IP connections from the network tunnel clients.

IP ADDRESS POOLS

Address pools are used to allocate IP addresses to the network tunnel clients. When configuring a community, you must specify which address pools are available to users.

□	TYPE	NAME	DESCRIPTION	USED
□		BVT EVPN pool	Address Pool	

WEB RESOURCE FILTERING

Web resource filtering enables extra processing for defined IP addresses and ports to detect HTTP traffic. When HTTP requests are found, policy and single sign-on logic are applied to the web server connections.

Web resource filtering: Enabled

DEVICE VPN

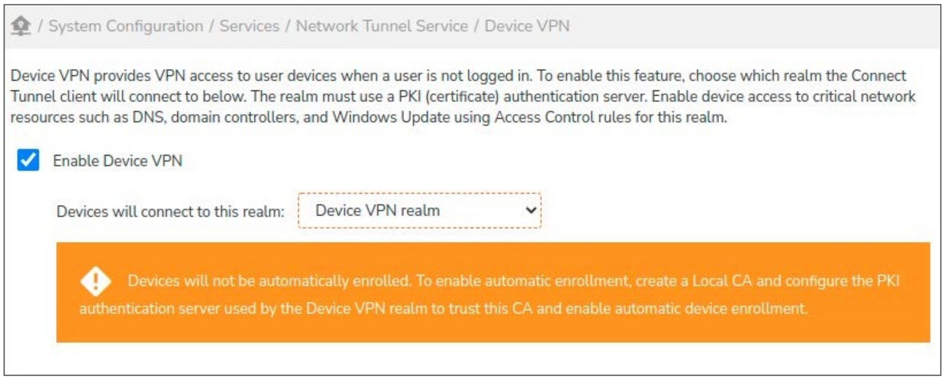
Device VPN provides VPN access to user devices when a user is not logged in. Device VPN is supported on Windows using the Connect Tunnel client. Device VPN can be used to enforce a persistent VPN connection for systems whether or not a user is currently logged in.

Device VPN: Disabled

CUSTOM CONNECTIONS

By default, Connect Tunnel is configured to access the realm and appliance from which it was downloaded. Use these options to configure Connect Tunnel to access a different default appliance or realm, or list other appliances and realms the client can connect to.

4. Select the **Enable Device VPN** checkbox and choose the realm from the drop-down to which you want to connect the devices.



/ System Configuration / Services / Network Tunnel Service / Device VPN

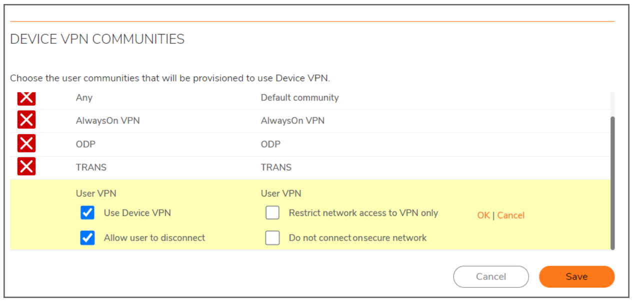
Device VPN provides VPN access to user devices when a user is not logged in. To enable this feature, choose which realm the Connect Tunnel client will connect to below. The realm must use a PKI (certificate) authentication server. Enable device access to critical network resources such as DNS, domain controllers, and Windows Update using Access Control rules for this realm.

☑ Enable Device VPN

Devices will connect to this realm: Device VPN realm

Devices will not be automatically enrolled. To enable automatic enrollment, create a Local CA and configure the PKI authentication server used by the Device VPN realm to trust this CA and enable automatic device enrollment.

5. In the **Device VPN Communities** group, select the user communities that needs to be provisioned to use the Device VPN. The selected communities alone can access the Device VPN.



DEVICE VPN COMMUNITIES

Choose the user communities that will be provisioned to use Device VPN.

☒	Any	Default community
☒	AlwaysOn VPN	AlwaysOn VPN
☒	ODP	ODP
☒	TRANS	TRANS
	User VPN ☑ Use Device VPN ☑ Allow user to disconnect	User VPN ☐ Restrict network access to VPN only ☐ Do not connect onsecure network

a. Set the User VPN options as required:

Options	Description
Use Device VPN	To enable Device VPN for this Community.
Allow user to disconnect	To allow user to disconnect from current session. **NOTE:** This setting takes precedence over **Always On VPN** configuration.
Restrict network access to VPN	To restrict network access to the users until VPN is completely connected.
Do not connect on secure network	To enable users to bypass entering VPN credentials for User VPN, when the client machine is powered on or restarts in secure network.

b. Click **OK**.

6. Click **Save**.

Viewing and Deleting or Revoking Device VPN certificate

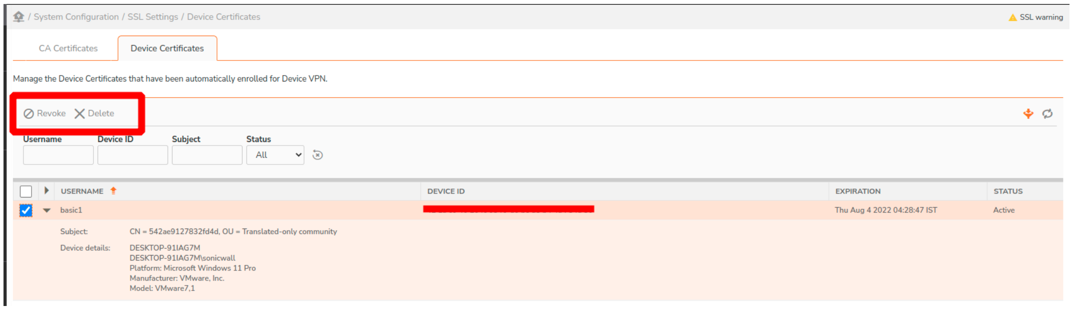
1. Go to **System Configuration** > **SSL Settings** > **Under CA certificate** .

2. Click **Edit** .

   The **Device Certificate** page is displayed. You can view the enrolled device certificate details using filters.

3. Select the required device certificate and you can do the following:
   - Click **Revoke**.

     Or
   - Click **Delete**.



Manage the Device Certificates that have been automatically enrolled for Device VPN.

☐	USERNAME	DEVICE ID	EXPIRATION	STATUS
☑	basic1	[redacted]	Thu Aug 4 2022 04:28:47 IST	Active

Subject: CN = 542ae9127832fd4d, OU = Translated-only community

Device details: DESKTOP-91IAG7M
DESKTOP-91IAG7M\sonicwall
Platform: Microsoft Windows 11 Pro
Manufacturer: VMware, Inc.
Model: VMware7,1

ⓘ **NOTE:** When you revoke or delete the device certificate, the device VPN session is disconnected and the client is re-enrolled or re-connects device VPN for the next successful User VPN authentication.

Configuring Custom Connections

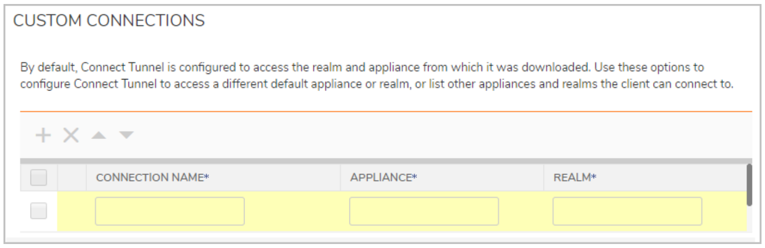
By default, Connect Tunnel is configured to access the realm and appliance from which it was downloaded. Use the Custom Connections options to configure Connect Tunnel to access a different default appliance or realm, or list other appliances and realms the client can connect to.

To configure custom connections:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Network tunnel service** area, Configure.

   The **Network Tunnel Service** page displays.
3. In the **Custom Connections** section, click the **+** (New) icon.
4. Select the type of connection from the dropdown list:
   - **Connection to this appliance**
   - **Connection to a different appliance**

   The **Custom connections** table displays editable fields for the connection name, appliance, and realm.



By default, Connect Tunnel is configured to access the realm and appliance from which it was downloaded. Use these options to configure Connect Tunnel to access a different default appliance or realm, or list other appliances and realms the client can connect to.

☐	CONNECTION NAME*	APPLIANCE*	REALM*
☐			

5. Type a descriptive name for the custom connection into the **Connection name** field.
6. Type the FQDN or IP address of the appliance into the **Appliance** field.

7. Type the realm name into the **Realm** field.
8. Select **Display** notifications checkbox if notifications should be displayed when this custom connection is used.
9. Select **Prompt for reconnect** checkbox if the user should be prompted to reconnect to this custom connection if disconnected.
10. Click **OK**.
11. When more than one custom connection is listed, to change the order of the connections, select the checkbox next to one custom connection and then click either **Move Up** or **Move Down**. The list is updated with the new order.
12. To delete a custom connection, select the checkbox next to it and then click **Delete**.

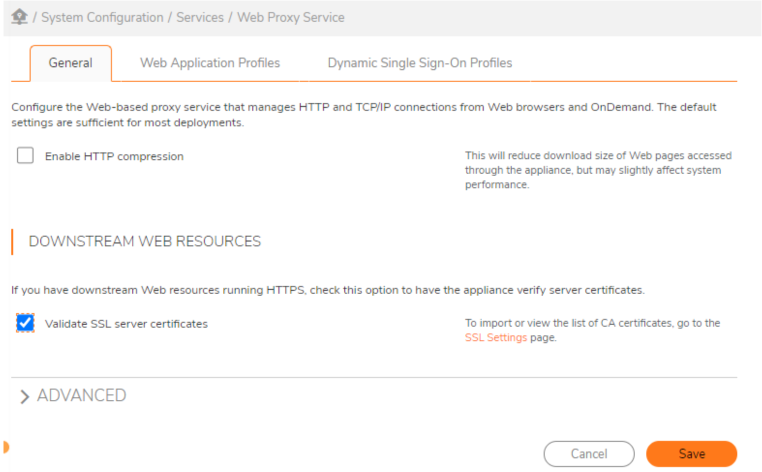
Configuring the Web Proxy Service

This section describes how to configure the service that manages access to Web resources. The Web proxy service provides Web proxy access, translated Web access, custom port mapped Web access, and custom FQDN mapped Web access.

To configure the Web proxy service:

1. In the AMC, navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **Web proxy service** area, **Configure**.

   The **Web Proxy Service** page displays.


/ System Configuration / Services / Web Proxy Service
General
Web Application Profiles
Dynamic Single Sign-On Profiles
DOWNSTREAM WEB RESOURCES
> ADVANCED
Cancel
Save

Configure the Web-based proxy service that manages HTTP and TCP/IP connections from Web browsers and OnDemand. The default settings are sufficient for most deployments.

□ Enable HTTP compression

This will reduce download size of Web pages accessed through the appliance, but may slightly affect system performance.

If you have downstream Web resources running HTTPS, check this option to have the appliance verify server certificates.

☑ Validate SSL server certificates

To import or view the list of CA certificates, go to the SSL Settings page.

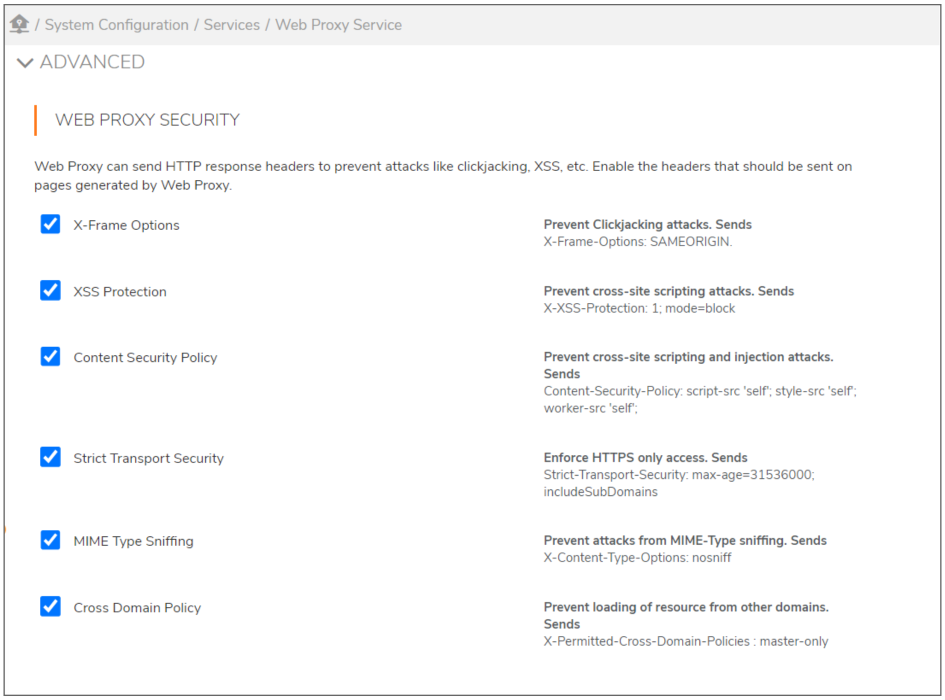
3. On the **General** tab, select **Enable HTTP compression** if you want to compress HTML, XML, and CSS files before they are sent from the appliance to the client. This reduces the download size of Web pages accessed through the appliance, but may also affect system performance.

   Enabling compression may affect system performance.
4. Configure **Downstream Web resources**:

- If you want the Web proxy service to check the validity of certificates presented by back-end Web servers, select **Validate SSL server certificates**. If enabled, the appliance will make sure the CN in the certificate matches the host name and that the certificate is valid. Secure Mobile Access recommends enabling this feature if you are using downstream HTTPS.
- To view details about the appliance's root certificate listing CAs that issued certificates to back-end Web servers, or to import a certificate, click **the SSL Settings** link. For more information about managing CA certificates, see CA Certificates.

ⓘ | **NOTE:** For information about configuring Web application profiles, see Adding Web Application Profiles.

5. Click **Advanced** to configure the **Web Proxy Security** settings.



/ System Configuration / Services / Web Proxy Service

ADVANCED

WEB PROXY SECURITY

Web Proxy can send HTTP response headers to prevent attacks like clickjacking, XSS, etc. Enable the headers that should be sent on pages generated by Web Proxy.

☑ X-Frame Options — **Prevent Clickjacking attacks. Sends** X-Frame-Options: SAMEORIGIN.

☑ XSS Protection — **Prevent cross-site scripting attacks. Sends** X-XSS-Protection: 1; mode=block

☑ Content Security Policy — **Prevent cross-site scripting and injection attacks. Sends** Content-Security-Policy: script-src 'self'; style-src 'self'; worker-src 'self';

☑ Strict Transport Security — **Enforce HTTPS only access. Sends** Strict-Transport-Security: max-age=31536000; includeSubDomains

☑ MIME Type Sniffing — **Prevent attacks from MIME-Type sniffing. Sends** X-Content-Type-Options: nosniff

☑ Cross Domain Policy — **Prevent loading of resource from other domains. Sends** X-Permitted-Cross-Domain-Policies : master-only

6. Select the headers to be sent on pages generated by Web Proxy. These headers protect users from attacks like Clickjacking and cross-site scripting.

ⓘ | **NOTE:** It is recommended to enable all the security headers for better security.

Header	Description
X-Frame Options	Prevent Clickjacking attacks: This header inspects and provides clickjacking protection by not allowing rendering of a page in a frame.
X-XSS-Protection	Prevent cross-site scripting and injection attacks: Using this header stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.
Content-Security-Policy	Prevent cross-site scripting and injection attacks: Using this header in modern browsers helps to enhance the security of the document (or web page).

Header	Description
Strict-Transport-Security	Enforce HTTPS only access: This header informs browsers that the site should only be accessed using HTTPS, and that any future attempts to access it using HTTP should automatically be converted to HTTPS.
MIME-Type Sniffing	Prevent attacks from MIME-Type sniffing: This header allows you to avoid MIME type sniffing by saying that the MIME types are deliberately configured.
Cross Domain Policy	Prevent loading of resource from other domains: This header is used to permit cross-domain requests from PDF documents.

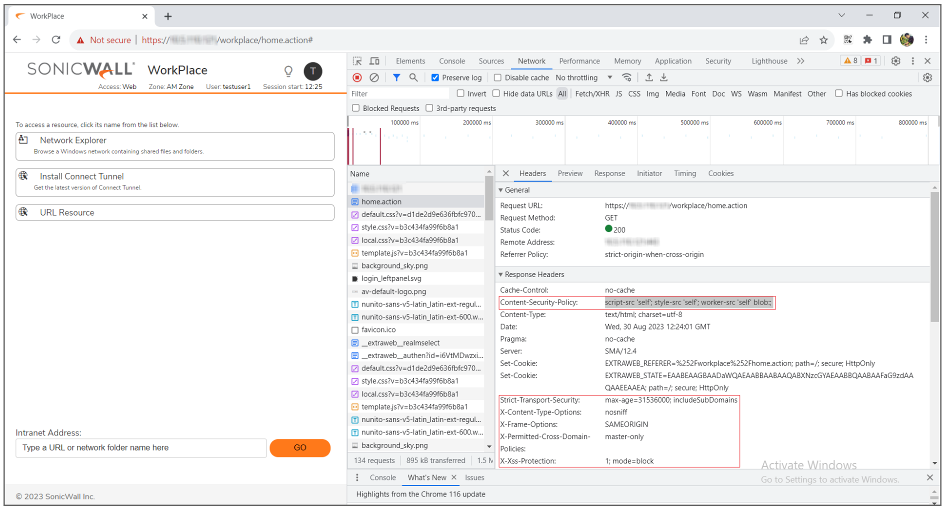
7. Click **Save**.

Verifying the Web Proxy Security headers

To verify the web proxy security headers:

1. Login to Workplace.
2. Check the Workplace requests generated by Web Proxy and verify the response headers sent for these requests.

   The requests contain the HTTP Response Headers enabled in AMC.



WorkPlace
Not secure
https://[redacted]/workplace/home.action#
SONICWALL
WorkPlace
Access: Web Zone: AM Zone User: testuser1 Session start: 12:25
To access a resource, click its name from the list below.
Network Explorer
Browse a Windows network containing shared files and folders.
Install Connect Tunnel
Get the latest version of Connect Tunnel.
URL Resource
Intranet Address:
Type a URL or network folder name here
GO
© 2023 SonicWall Inc.
Elements Console Sources Network Performance Memory Application Security Lighthouse
☑ Preserve log □ Disable cache No throttling
Filter □ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies
□ Blocked Requests □ 3rd-party requests
100000 ms 200000 ms 300000 ms 400000 ms 500000 ms 600000 ms 700000 ms 800000 ms
Name
[redacted]
home.action
default.css?v=d1de2d9e636fbfc970...
style.css?v=b3c434fa99f6b8a1
local.css?v=b3c434fa99f6b8a1
template.js?v=b3c434fa99f6b8a1
background_sky.png
login_leftpanel.svg
av-default-logo.png
nunito-sans-v5-latin_latin-ext-regul...
nunito-sans-v5-latin_latin-ext-600.w...
favicon.ico
__extraweb__realmselect
__extraweb__authen?id=i6VtMDwzxi...
default.css?v=d1de2d9e636fbfc970...
style.css?v=b3c434fa99f6b8a1
local.css?v=b3c434fa99f6b8a1
template.js?v=b3c434fa99f6b8a1
nunito-sans-v5-latin_latin-ext-regul...
nunito-sans-v5-latin_latin-ext-600.w...
background_sky.png
134 requests 895 kB transferred 1.5 M
Headers Preview Response Initiator Timing Cookies
Console What's New Issues
Highlights from the Chrome 116 update
Activate Windows
Go to Settings to activate Windows.

▾ General

Request URL: https://[redacted]/workplace/home.action
Request Method: GET
Status Code: ● 200
Remote Address: [redacted]
Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers

```
Cache-Control:                  no-cache
Content-Security-Policy:        script-src 'self'; style-src 'self'; worker-src 'self' blob:;
Content-Type:                   text/html; charset=utf-8
Date:                           Wed, 30 Aug 2023 12:24:01 GMT
Pragma:                         no-cache
Server:                         SMA/12.4
Set-Cookie:                     EXTRAWEB_REFERER=%252Fworkplace%252Fhome.action; path=/; secure; HttpOnly
Set-Cookie:                     EXTRAWEB_STATE=EAABEAAGBAADaWQAEAABBAABAAQABXNzcGYAEAABBQAABAAFaG9zdAA
                                QAAEEAAEA; path=/; secure; HttpOnly
Strict-Transport-Security:      max-age=31536000; includeSubDomains
X-Content-Type-Options:         nosniff
X-Frame-Options:                SAMEORIGIN
X-Permitted-Cross-Domain-
Policies:                       master-only
X-Xss-Protection:               1; mode=block
```

Terminal Server Access

The SMA appliance supports native Web-based access to individual Windows Terminal Services or Citrix servers, and to Citrix server farms.

Topics:

Providing Access to Terminal Server Resources

The Web-based graphical terminal agents provide access to a terminal server using native application protocols. For example, when accessing a Citrix server, the client sends traffic from the client to the server using the proprietary (non-HTTP) Citrix protocol. Accordingly, to provide access to a terminal server resource, you must configure WorkPlace to provision one of the Secure Mobile Access access methods using one of the tunnel clients. If you configure WorkPlace to provide only Translated Web access, terminal resources will be unavailable because the client computer will not have the network transport required to access a proprietary application protocol. For information about configuring access methods, see Selecting Tunnel Access Methods for a Community.

You can enable single sign-on for applications hosted on Windows Terminal Services or a Citrix server; this passes the user’s WorkPlace login credentials to all published applications on the server. If you disable single sign-on, an additional login page is displayed and the user must supply the required credentials before accessing any applications that are hosted on the terminal server.

Enabling access to terminal server resources consists of these basic steps:

1. Define the terminal server resources and access policy

   First define individual Windows Terminal Services or Citrix servers, or Citrix server farms, and then add these resources to access control rules:

   - You must define each host or Citrix server farm object as a resource in AMC. If your network includes a set of Citrix servers that have similar names, you can save time by using wildcard characters to define one resource object that includes multiple servers.

     If you are configuring a Citrix server farm, you must also define each individual Citrix server that is hosting applications as a resource. For information about defining Citrix server farms, see Adding Citrix Server Farm Resources.

   - Reference the resources in access control rules as you would any other resource. For information about providing terminal server access to individual Windows Terminal Services or Citrix servers, and see Defining an Access Control Rule and Resource for Terminal Server Access.

2. Install or update the appropriate graphical terminal agent

   When a user initiates a connection to a Citrix or Windows Terminal Services resource through WorkPlace, the appliance determines whether the version of the applicable agent that is available on the appliance is already installed on the user’s computer, and automatically installs or updates the agent as needed. You must ensure that the correct graphical terminal agents are configured in AMC; for information about managing the agents, see Managing Graphical Terminal Agents.

3. Create a WorkPlace shortcut that references the terminal server resource

   The Windows Terminal Services or Citrix host is accessed from a Web-based agent that is deployed when users click a shortcut in WorkPlace. For information about configuring graphical terminal WorkPlace shortcuts, see Graphical Terminal Shortcuts.

Server Farm Resources

The SMA appliance allows you to specify individual Citrix servers, one or more load-balanced Citrix server farms, or VMware servers.

Topics:

- Adding Citrix Server Farm Resources
- Adding VMware View Resources

Adding Citrix Server Farm Resources

This section describes how to define a Citrix server farm as a resource. For information about providing terminal server access to Citrix servers, see Defining an Access Control Rule and Resource for Terminal Server Access.

To enable users to access Citrix resources, first configure the appliance with two Citrix agents: an ActiveX control that runs on Windows, and a cross-platform Java applet. Once the agent files are uploaded to the appliance, the appropriate Citrix client is automatically provisioned to users the first time they access a Citrix resource from WorkPlace. For details, see Managing Graphical Terminal Agents. The appliance supports all desktop operating systems and applications that are supported by the Citrix clients. Small form factor devices are not supported.

For individual Citrix servers, you can specify a custom ICA file; these files contain additional configuration settings for the Citrix host.

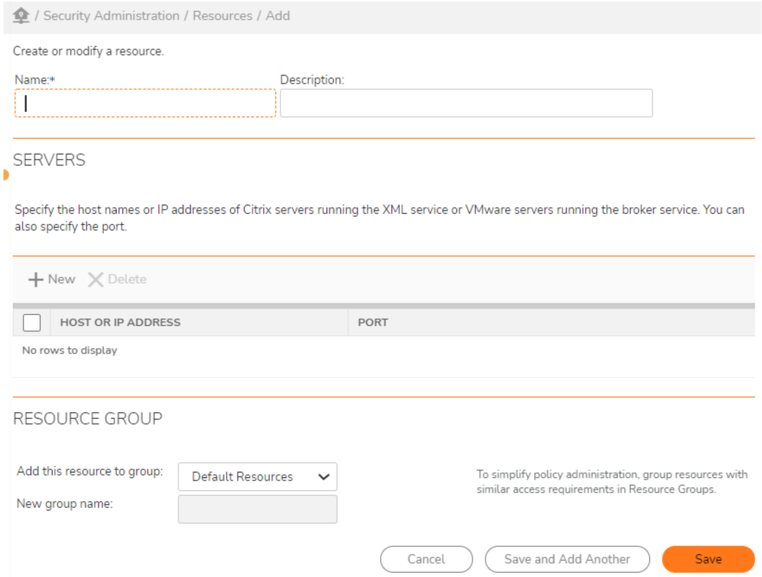
Citrix server farms must meet the following system requirements:

- Citrix XenApp
- Citrix XML service must be running

When a user clicks a WorkPlace shortcut that points to a Citrix server farm, a separate WorkPlace window appears and displays the resources that are hosted on the server. The WorkPlace Web interface provides the services that users need to browse and work with applications that are hosted on Citrix servers in the farm. There is no need to deploy an additional Web interface. The user can browse these resources and click links to automatically launch applications. The Citrix applications appear in the Citrix client window.

To add a Citrix server farm resource:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon.
3. Select **Server farm** from the dropdown list. The **Add Resource - Server Farm** page displays.



Create or modify a resource.

Name:*

Description:

SERVERS

Specify the host names or IP addresses of Citrix servers running the XML service or VMware servers running the broker service. You can also specify the port.

□	HOST OR IP ADDRESS	PORT

No rows to display

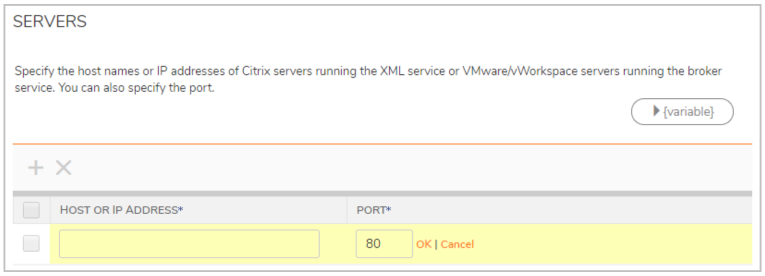
RESOURCE GROUP

Add this resource to group: Default Resources

New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

4. In the **Name** field, type a name for the server farm.
5. In the **Description** field, type a descriptive comment about the server farm. This step is optional, but a description can be helpful later when viewing your list of resources.
6. Under **Servers**, click the **+** (New) icon.
7. Specify the servers that are included in the server farm. Each server farm must include at least one Citrix XenApp server.



SERVERS

Specify the host names or IP addresses of Citrix servers running the XML service or VMware/vWorkspace servers running the broker service. You can also specify the port.

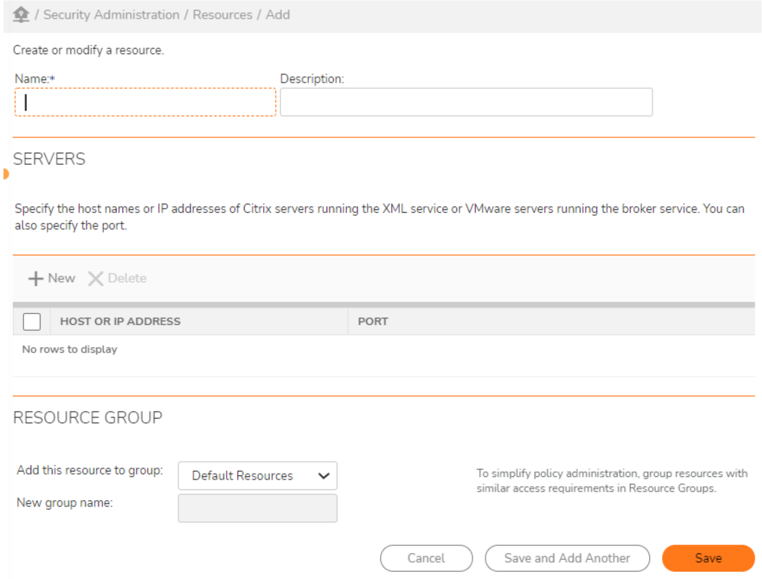
□	HOST OR IP ADDRESS*	PORT*
□		80 OK | Cancel

   a. In the **Host or IP address** field, type the host name or IP address for the Citrix XenApp server.
   b. In the **Port** field, type the number of the port through which the appliance connects to the XML browser service on the Citrix XenApp server. The default port number is **80**.
   c. Click **OK**. The server is added to the list of servers in the farm.
8. Click **Save**.

Adding VMware View Resources

To add a VMware view resource:

1. In the AMC, navigate to **Security Administration > Resources**.
2. Click the **+** (New) icon.
3. Select **Server farm** from the dropdown list. The **Add Resource - Server Farm** page displays.



Create or modify a resource.

Specify the host names or IP addresses of Citrix servers running the XML service or VMware servers running the broker service. You can also specify the port.

No rows to display

To simplify policy administration, group resources with similar access requirements in Resource Groups.

4. In the **Name** field, type a name for the VMware view.
5. Optional. In the **Description** field, type a descriptive comment about the VMware view.
6. Under **Citrix or VMware servers**, click **New** and then specify the VMware servers that are included in the VMware view. Each view must include at least one server.
   a. In the **Host or IP address** field, type the host name or IP address for the VMware server.
   b. In the **Port** field, type the number of the port through which the appliance connects to the service on the VMware server. The default port number is *80*.
   c. Click **OK**.
7. Click **Save**.

To add a VMware View Client:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. In the **Other Agents** section, click **Configure** next to **Graphical terminal agents**.
3. In the **VMware View clients** section, click **Browse...** to navigate to the agent file. Select the agent file for each client.
4. Click **Save**.

Browser-Only Mode for Citrix Access

Citrix has developed HTML browser-based receivers which can be used from browsers to connect to XenApp and XenDesktop. SMA provides an easy way to configure Citrix HTML receivers from the SMA appliance to enable end users to access these backend applications easily.

By leveraging the Citrix HTML based receiver, administrators can configure the Citrix StoreFront URL in the appliance as a URL Resource. Users can then launch the URL through host mapped or port mapped methods (reverse proxy), provide their credentials, and get redirected to the HTML view of StoreFront.

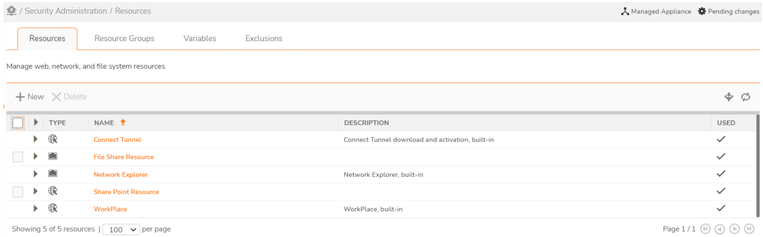
Topics:

- Configuring the Citrix HTML Receiver URL
- Configuring a Shortcut for Citrix HTML Receiver in Workplace

Configuring the Citrix HTML Receiver URL

To configure the URL for the Citrix HTML Receiver:

1. In the AMC, navigate to **Security Administration > Resources**.

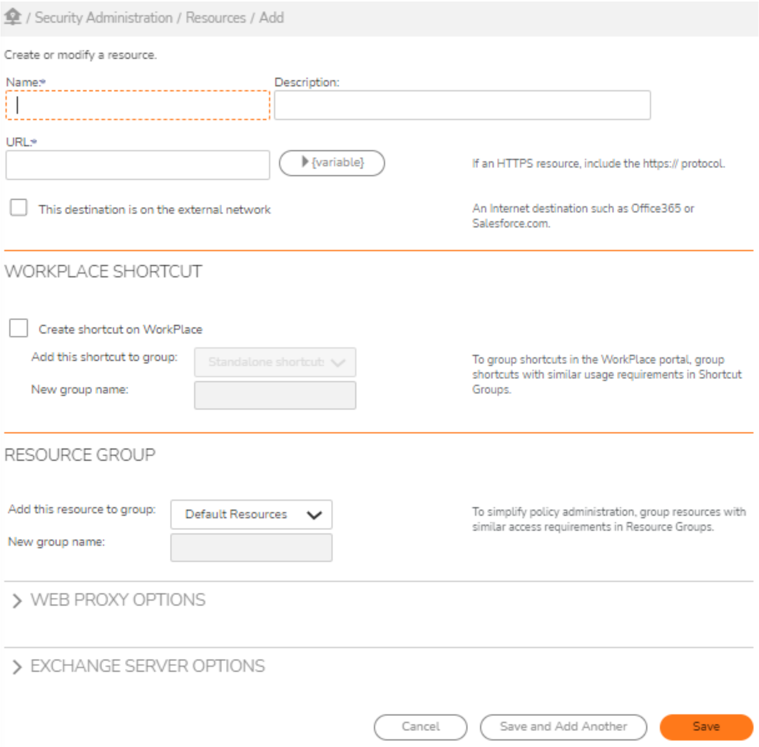


Manage web, network, and file system resources.

TYPE	NAME	DESCRIPTION	USED
	Connect Tunnel	Connect Tunnel download and activation, built-in	✓
	File Share Resource		✓
	Network Explorer	Network Explorer, built-in	✓
	Share Point Resource		✓
	WorkPlace	WorkPlace, built-in	✓

Showing 5 of 5 resources | 100 per page   Page 1 / 1

2. Click the **+** (New) icon.
3. Select **URL** from the dropdown list. The **Add Resource - URL** page displays.



/ Security Administration / Resources / Add

Create or modify a resource.

Name:*

Description:

URL:*

{variable}

If an HTTPS resource, include the https:// protocol.

□ This destination is on the external network

An Internet destination such as Office365 or Salesforce.com.

WORKPLACE SHORTCUT

□ Create shortcut on WorkPlace

Add this shortcut to group: Standalone shortcut

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

RESOURCE GROUP

Add this resource to group: Default Resources

New group name:

To simplify policy administration, group resources with similar access requirements in Resource Groups.

> WEB PROXY OPTIONS

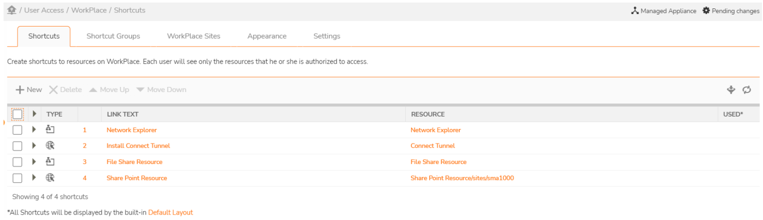
> EXCHANGE SERVER OPTIONS

4. In the **Name** field, enter the name for this URL resource, such as Citrix HTML Receiver.
5. In the **URL** field, enter the URL of the Citrix HTML Receiver.
6. If this resource is on the external network, select the checkbox for **This destination is on the external network**.
7. Select the **Create Shortcut on WorkPlace** checkbox.
8. In the **Custom access** panel, from the drop-down menu, select **Access this resource on a custom port**.
9. In the **Port** field, enter the port number you want.
10. Click **Save**.

Configuring a Shortcut for Citrix HTML Receiver in Workplace

To configure a shortcut for the Citrix HTML Receiver in Workplace:

1. In the AMC, navigate to **User Access > Workplace**.
2. Click the **Shortcuts** tab.



/ User Access / WorkPlace / Shortcuts

Create shortcuts to resources on WorkPlace. Each user will see only the resources that he or she is authorized to access.

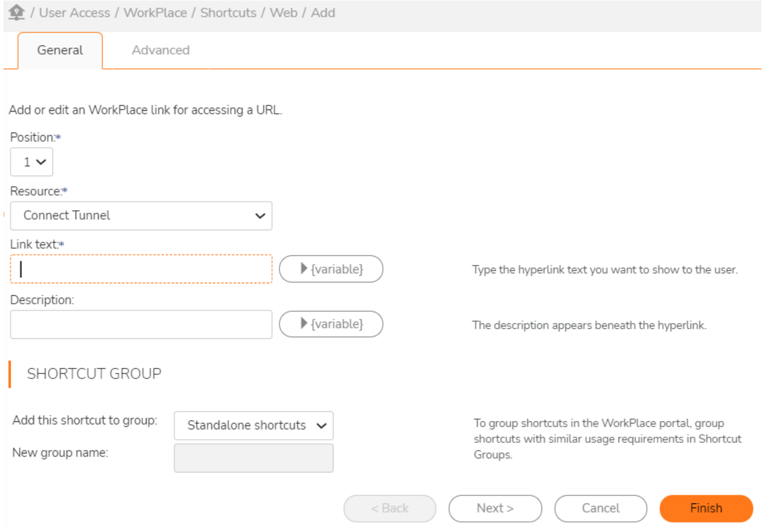
TYPE		LINK TEXT	RESOURCE	USED*
	1	Network Explorer	Network Explorer	
	2	Install Connect Tunnel	Connect Tunnel	
	3	File Share Resource	File Share Resource	
	4	Share Point Resource	Share Point Resource/sites/sma1000	

Showing 4 of 4 shortcuts

*All Shortcuts will be displayed by the built-in Default Layout

3. Click the **+** (New) icon.

4. Select **Web shortcut** from the dropdown list. The **Add Web Shortcut** page displays.



/ User Access / WorkPlace / Shortcuts / Web / Add

Add or edit an WorkPlace link for accessing a URL.

Position:* 1

Resource:* Connect Tunnel

Link text:*

Type the hyperlink text you want to show to the user.

Description:

The description appears beneath the hyperlink.

SHORTCUT GROUP

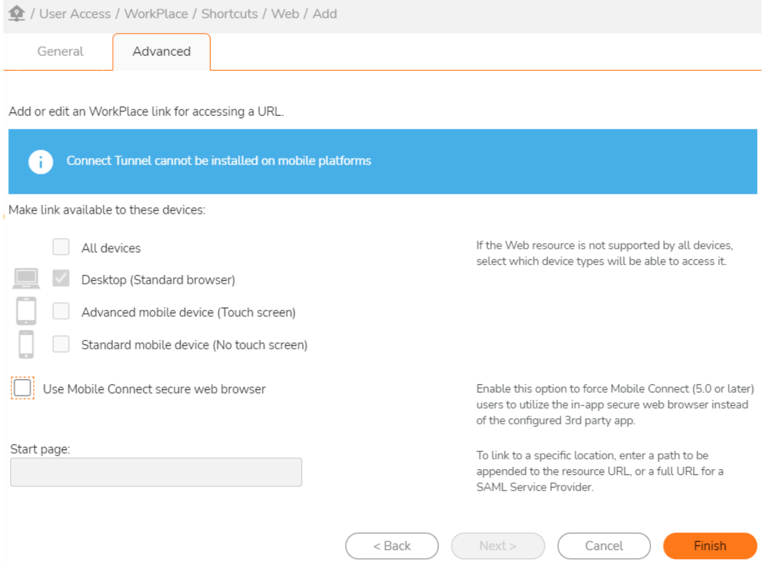
Add this shortcut to group: Standalone shortcuts

New group name:

To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

5. Enter the name and description of the Citrix HTML Receiver in the appropriate fields.

6. Click **Next** to display the **Advanced** page.



/ User Access / WorkPlace / Shortcuts / Web / Add

Add or edit an WorkPlace link for accessing a URL.

Connect Tunnel cannot be installed on mobile platforms

Make link available to these devices:

☐ All devices

☑ Desktop (Standard browser)

☐ Advanced mobile device (Touch screen)

☐ Standard mobile device (No touch screen)

If the Web resource is not supported by all devices, select which device types will be able to access it.

☐ Use Mobile Connect secure web browser

Enable this option to force Mobile Connect (5.0 or later) users to utilize the in-app secure web browser instead of the configured 3rd party app.

Start page:

To link to a specific location, enter a path to be appended to the resource URL, or a full URL for a SAML Service Provider.

7. Select the **All devices** checkbox.
8. In the **Start page** field, enter URL of the Citrix HTML Receiver:

   `/citrix/store2web`
9. Click **Save**.

Defining an Access Control Rule and Resource for Terminal Server Access

This section describes how to provide terminal sever access to your users by defining an access control rule and creating a terminal server resource. For more information see, Access Control Rules and Adding Resources.

To define a terminal server resource:

1. In the AMC, navigate to **Security Administration > Access Control**.
2. Click the **+** (New) icon. The **Add Access Rule** page displays.
3. In the **Number** field, type a number to specify the rule's position in the access rule list.
4. Use the **Action** buttons to specify **Permit**.
5. Complete the information under **Basic settings**:
   a. Leave **User** selected (so that the rule applies to users trying to access a resource).
   b. The **From** field specifies the users to whom the rule applies. For this example, leave the value as *Any user*.
   c. In the **To** field, click **Edit** to specify the target resource for this rule. A **Resources** page displays.
   d. Click **New** and then select **Host name** or **IP** from the list. If you have more than one terminal server on the same IP subnet, you can select **IP range** or **Subnet**. The **Add/Edit Resource** page displays.
   e. Type a name for the resource. For example, `terminal server`.
   f. In the **Host name or IP address** field, type the host name or IP address for the terminal server.
   g. Click **Save**. The **Add/Edit Resource** page closes.
6. Click **Finish**.

Managing Graphical Terminal Agents

This section describes how to configure the graphical terminal agents that give users access to terminal server resources through the SMA appliance. For information about providing access to terminal servers through WorkPlace, see Graphical Terminal Shortcuts.

Topics:

- Managing the VMware View Clients

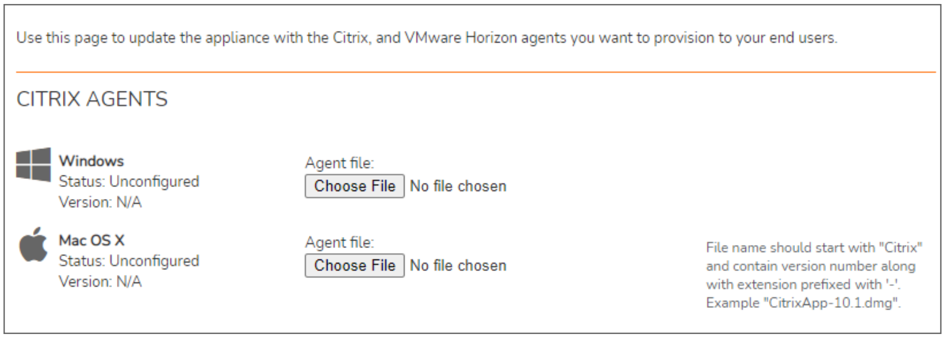
Managing the Citrix Agent

To enable users to access Citrix resources, you must configure the appliance with Citrix agent.

To configure the appliance for each Citrix agent, upload the agent file to the appliance. The SMA appliance provisions the Citrix agents to users the first time they access a Citrix resource from WorkPlace.

To install the Citrix agents:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. In the **Other Agents** section, click **Configure** next to **Graphical terminal agents**.
   The **Graphical Terminal Agents** page displays.



Use this page to update the appliance with the Citrix, and VMware Horizon agents you want to provision to your end users.

CITRIX AGENTS

Windows
Status: Unconfigured
Version: N/A

Agent file:
Choose File No file chosen

Mac OS X
Status: Unconfigured
Version: N/A

Agent file:
Choose File No file chosen

File name should start with "Citrix" and contain version number along with extension prefixed with '-'. Example "CitrixApp-10.1.dmg".

3. To specify the Windows agent, configure the **Windows** settings under **Citrix agents**:
   a. In the **Agent file** field, type the path for the agent file, or click **Browse** to locate it.
   b. Click **Save** to transfer the file to the SMA appliance.
4. To specify the macOS agent, configure the **Mac OS X** settings under **Citrix agents**:
   a. In the **Agent file** field, type the path for the agent file, or click **Browse** to locate it.
   b. Click **Save** to transfer the file to the SMA appliance.

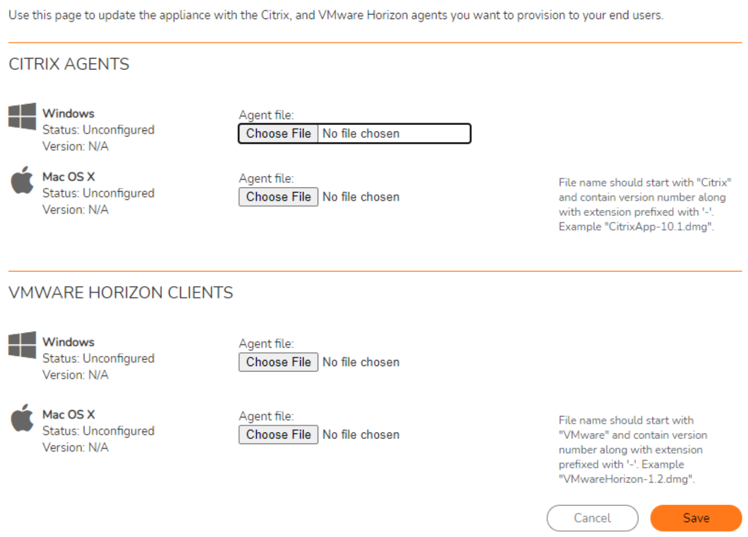
Managing the VMware View Clients

To enable Windows users to access VMware resources, you must configure the appliance with VMware View client.

To configure the appliance for each VMware View client, upload the agent file to the appliance. The SMA appliance provisions the VMware View agents to users the first time they access a VMware View resource from WorkPlace.

To install the VMware agents:

1. In the AMC, navigate to **User Access > Agent Configuration**.
2. In the **Other Agents** section, click **Configure** next to **Graphical terminal agents**.
   The **Graphical Terminal Agents** page displays.



Use this page to update the appliance with the Citrix, and VMware Horizon agents you want to provision to your end users.

CITRIX AGENTS

Windows
Status: Unconfigured
Version: N/A

Agent file: No file chosen

Mac OS X
Status: Unconfigured
Version: N/A

Agent file: No file chosen

File name should start with "Citrix" and contain version number along with extension prefixed with '-'. Example "CitrixApp-10.1.dmg".

VMWARE HORIZON CLIENTS

Windows
Status: Unconfigured
Version: N/A

Agent file: No file chosen

Mac OS X
Status: Unconfigured
Version: N/A

Agent file: No file chosen

File name should start with "VMware" and contain version number along with extension prefixed with '-'. Example "VMwareHorizon-1.2.dmg".

3. To specify the agent for a Windows VMware View client, configure the **Windows** settings under **VMWare View clients:**
   a. In the **Agent file** field, type the path for the agent file, or click **Browse** to locate it.
   b. Click **Save** to transfer the file to the SMA appliance.
4. To specify the agent for a macOS VMware View client, configure the **Mac OS X** area under **VMWare View clients:**
   a. In the **Agent file** field, type the path for the agent file, or click **Browse** to locate it.
   b. Click **Save** to transfer the file to the SMA appliance.

Graphical Terminal Shortcuts

Graphical terminal shortcuts provide your users with Web-based access to resources that are available through Windows Terminal Services or Citrix hosts. Before you can create a shortcut to a terminal resource, you must first define the resource (for more information, see Adding Resources and Adding Citrix Server Farm Resources). You must also ensure that the correct graphical terminal agents are configured in AMC; for more information see Managing Graphical Terminal Agents.

This section describes how to configure graphical terminal shortcuts to individual Citrix or Windows Terminal Services hosts, and Citrix server farms.

Topics:

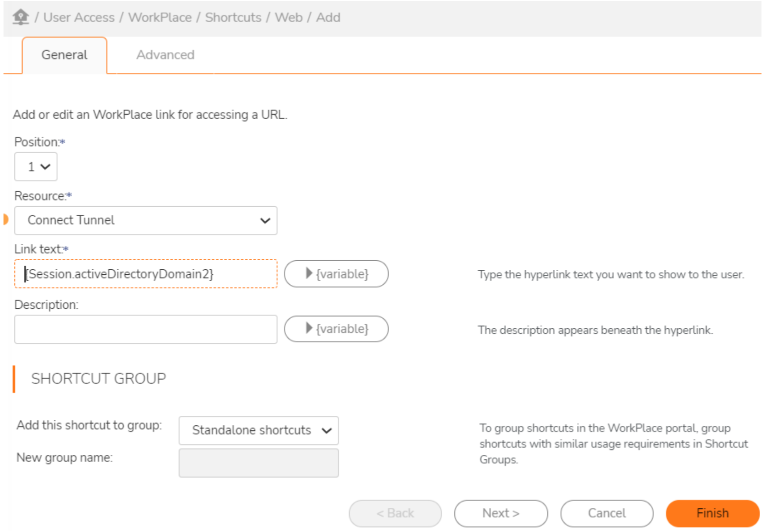
- Adding Graphical Terminal Shortcuts to Individual Hosts
- Adding Graphical Terminal Shortcuts to Server Farms

Adding Graphical Terminal Shortcuts to Individual Hosts

This section describes how to configure a graphical terminal shortcut to an individual Windows Terminal Services or Citrix host. For information about configuring graphical terminal shortcuts to Citrix server farms, see Adding Graphical Terminal Shortcuts to Server Farms.

To add a graphical terminal shortcut to an individual host:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts** tab.
3. Click the **+** (New) icon.
4. Select **Graphical terminal shortcut** from the dropdown list. The **Add Graphical Terminal Shortcut** page displays.



Add or edit an WorkPlace link for accessing a URL.

Position:* 1

Resource:* Connect Tunnel

Link text:* {Session.activeDirectoryDomain2}

Type the hyperlink text you want to show to the user.

Description:

The description appears beneath the hyperlink.

SHORTCUT GROUP

Add this shortcut to group: Standalone shortcuts

New group name:

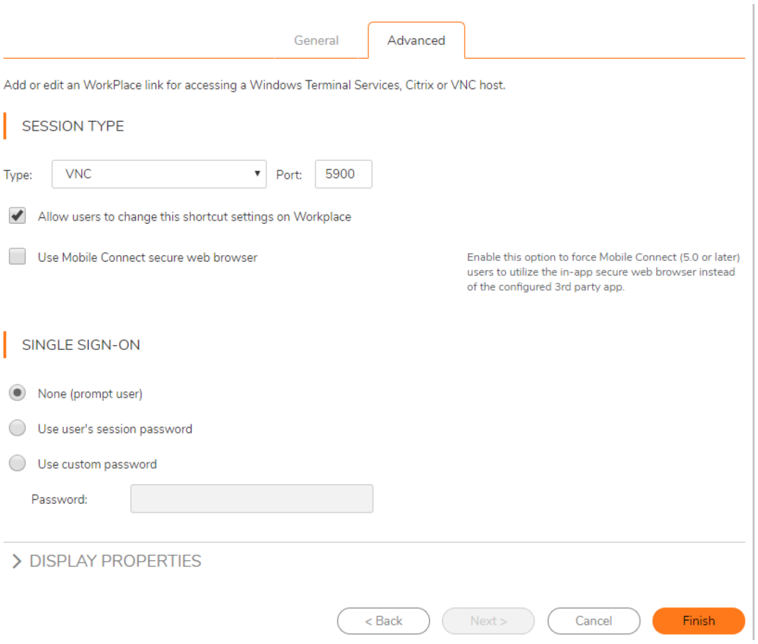
To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

5. In the **Position** field, specify the position of the shortcut in the list.
6. In the **Resource** drop-down menu, select the host or IP address resource to which this shortcut will be linked. This menu contains the available defined resources. (**URL** and **Network share** resources do not appear because they cannot have graphical terminal shortcuts associated with them.)
7. Enter the hyperlink that users will click to access the resource and (optionally) a description of the link that will appear next to it. These entries can include variables:
    a. In the **Link text** field, type the text for the hyperlink users will see. For example, if the resource you selected was the Windows domain for users' home directories, enter `Home directory`. Using a variable you can have the link be followed by the actual path: click **{variable}**, and then select **{URL_REF_VALUE}** from the list. Click **Insert** to add the variable to the link text, and then close the list by clicking **{variable}** again.
    b. In the **Description** field, type a descriptive comment about the shortcut. Although optional, a description helps users understand what the resource is. You can, for example, use a variable to be specific about the user's identity. Here's a sample entry for **Description**, followed by the

explanatory text the user (in this case *LGeorge*) sees in WorkPlace:

```
{Session.userName}'s user directory –> LGeorge's user directory
```

8. Click **Finish** to save the shortcut with the current settings, or click **Next** to display additional configuration settings. The **Advanced** tab of the **Add Graphical Terminal Shortcut** page displays.



Add or edit an WorkPlace link for accessing a Windows Terminal Services, Citrix or VNC host.

SESSION TYPE

Type: VNC Port: 5900

☑ Allow users to change this shortcut settings on Workplace

□ Use Mobile Connect secure web browser

Enable this option to force Mobile Connect (5.0 or later) users to utilize the in-app secure web browser instead of the configured 3rd party app.

SINGLE SIGN-ON

● None (prompt user)

○ Use user's session password

○ Use custom password

Password:

9. Under **Session type**, specify the type of session to initiate:

   - Click **Windows Terminal Services** to initiate a connection to a Windows Terminal Services host. In the **Port** field, type the port number for the Windows Terminal Services connection. Select the **Automatically reconnect if session is interrupted** checkbox for seamless reconnection attempts.
   - Click **Citrix** to initiate a connection to an individual Citrix host. In the **Port** field, type the port number for the connection. Optionally, you can specify a **Custom ICA file** by typing its path or clicking **Browse** to locate it. Custom ICA files contain additional configuration settings for the Citrix host.

10. Under **Single sign-on**, specify how you want user credentials forwarded to the host. Forwarding user credentials prevents the user from needing to log in multiple times (once to get to the appliance, and again to access the host).

    - Click **None** to disable single sign-on and instead prompt the user for credentials.
    - Click **Forward user's session credentials** to pass the username and password for authentication in WorkPlace along to the host.
    - Click **Forward static credentials** to forward the same username and password for all users. Type the static **Username**, **Password**, and **Domain** to be forwarded for all users.

11. Specify **Startup options** if you want to automatically start an application when users click the graphical terminal shortcut.

- In the **Start application** field, type the path to the application.
- If the application requires a working directory, type its path in the **Working directory** box.

12. Specify **Display properties:**

    - In the **Screen resolution** drop-down menu, select the appropriate resolution for the application. The default resolution is **1024 x 768 pixels**. To set a custom resolution, select **Custom...**, and then type the desired pixel values (width x height) into the fields that appear to the right. The minimum supported resolution is 640x480 and the maximum is 4096x2048 pixels.
    - For **Terminal Services** shortcuts, select the **Allow users to select a different resolution** checkbox to give users control over their screen resolution. Users will be able to select their own resolution from a list box on the shortcut itself in Workplace. This checkbox is disabled for Citrix shortcuts.
    - In the **Color depth** list, select the color depth. The default setting is **Lowest (8-bit)**.

      ⓘ | **NOTE:** Higher color depth settings can affect performance.

13. Specify **Resource redirection** settings as needed:

    - Select the **Allow access to local drives** checkbox to enable users to access local drives during the session.
    - Select the **Allow access to local printers** checkbox to enable users to access local printers during the session.
    - Select the **Bring remote audio to local computer** checkbox to enable users to access remote audio during the session. Note that audio redirection is network intensive and can affect performance. The default is off.
    - Select the **Share clipboard between local and remote computers** checkbox to enable clipboard copy/paste in both directions for the user. The default is to allow this feature.

14. Click **Finish**.

ⓘ | **NOTE:**

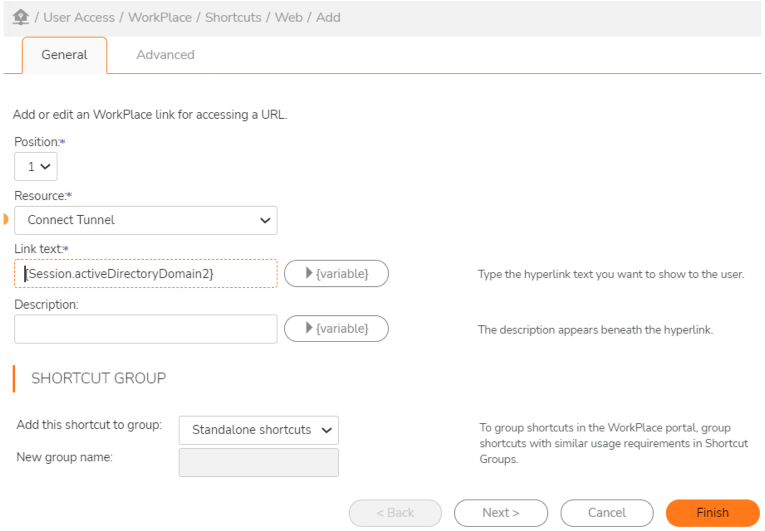
- Enabling single sign-on for shortcuts to Citrix hosts causes users' authentication credentials to be forwarded to the client, which can potentially compromise security.
- The Java open-source version of the Windows Terminal Services agent does not support any **Resource redirection** options.
- Enabling clipboard sharing is not appropriate for shortcut that provides read-only access to applications and sets of data.

Adding Graphical Terminal Shortcuts to Server Farms

This section describes how to configure a graphical terminal shortcut to a Citrix server farm. For information about configuring graphical terminal shortcuts to individual Citrix or Windows Terminal Services hosts, see Adding Graphical Terminal Shortcuts to Individual Hosts.

To add a graphical terminal shortcut to a server farm:

1. In the AMC, navigate to **User Access > WorkPlace**.
2. Click on the **Shortcuts** tab.
3. Click the **+** (New) icon.
4. Select **Graphical terminal shortcut** from the dropdown list. The **Add Graphical Terminal Shortcut** page displays.



Add or edit an WorkPlace link for accessing a URL.

Position:* 1

Resource:* Connect Tunnel

Link text:* {Session.activeDirectoryDomain2}

Type the hyperlink text you want to show to the user.

Description:

The description appears beneath the hyperlink.

Add this shortcut to group: Standalone shortcuts

New group name:

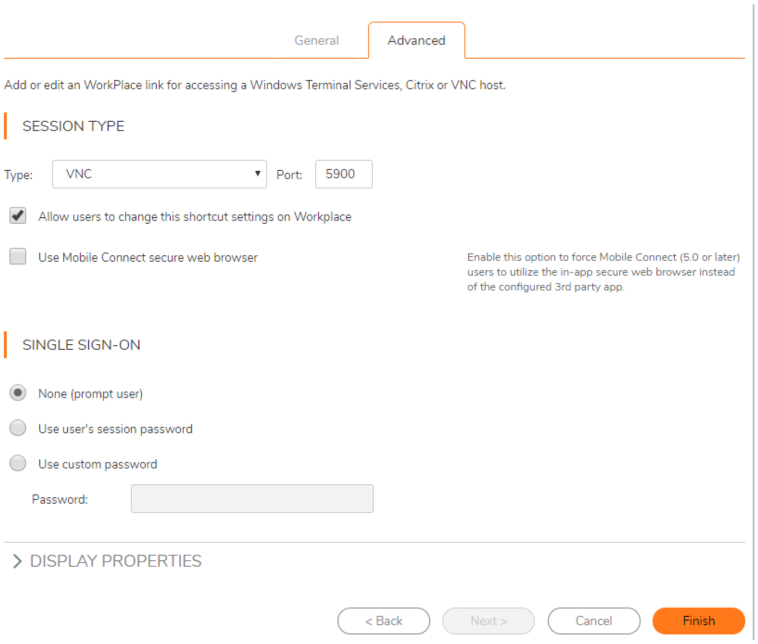
To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

5. In the **Position** field, specify the shortcut's position in the list.
6. In the **Resource** drop-down menu, select the resource to which this shortcut will be linked. This list contains the available defined resources. (**URL** and **Network share resources** do not appear because they cannot have graphical terminal shortcuts associated with them.)
7. In the **Link text** field, type the hyperlink text that users will click to access the graphical terminal resource.
8. Enter the hyperlink that users will click to access the resource and (optionally) a description of the link that will appear next to it. These entries can include variables:
   a. In the **Link text** field, type the text for the hyperlink users will see.
   b. In the **Description** field, type a descriptive comment about the shortcut. Although optional, a description helps users understand what the resource is. You can, for example, use a variable to be specific about the user's identity. Here's a sample entry for **Description**, followed by the explanatory text the user (in this case *LGeorge*) sees in WorkPlace:

      ```
      {Session.userName}'s user directory —> LGeorge's user directory
      ```

      In WorkPlace you can set up groups to organize resources for your users, or have shortcuts appear singly. In the **Shortcut group** area, add your new shortcut to a new or existing group, or have it appear on its own in WorkPlace by adding it to the Standalone shortcuts group. (The order in which shortcuts appear can be changed on the **Configure WorkPlace Layout** page; see Creating or Editing a WorkPlace Layoutfor more information.)

9. Click **Finish** to save the shortcut with the current settings, or click **Next** to display additional configuration settings. The **Advanced** tab of the **Add Graphical Terminal Shortcut** page displays.



Add or edit an WorkPlace link for accessing a Windows Terminal Services, Citrix or VNC host.

SESSION TYPE

Type: VNC Port: 5900

☑ Allow users to change this shortcut settings on Workplace

□ Use Mobile Connect secure web browser

Enable this option to force Mobile Connect (5.0 or later) users to utilize the in-app secure web browser instead of the configured 3rd party app.

SINGLE SIGN-ON

● None (prompt user)

○ Use user's session password

○ Use custom password

Password:

10. If necessary, you can specify a different **Port** for sending ICA traffic between the Citrix client and WorkPlace. The default port is **1494**.

11. Under **Single sign-on**, specify how you want user credentials forwarded to the host. Forwarding user credentials prevents the user from needing to log in multiple times (once to get to the appliance, and again to access the host).

    - Click **None** to disable single sign-on and instead prompt the user for credentials.
    - Click **Forward user's session credentials** to pass the username and password used for authentication in WorkPlace along to the host.
    - Click **Forward static credentials** to forward the same username and password for all users. Type the static **Username**, **Password**, and **Domain** to be forwarded for all users.

12. Select the **Enable SSO to Citrix applications** checkbox to forward the user's WorkPlace login credentials to all published applications that are hosted on the Citrix server farm. Enabling single sign-on to Citrix applications provides more convenience for the user; however, it can potentially compromise security, as users' passwords are temporarily stored in cleartext on the client computer.

13. Specify **Display properties:**

    - In the **Screen resolution** list, select the appropriate resolution for the application. The default setting is **1024 x 768 pixels**.
    - In the **Color depth** list, select the color depth. The default setting is **16-bit**.

      ⓘ | **NOTE:** Higher color depth settings can affect download speed.

14. Click **Save**.

NOTE: Enabling single sign-on for shortcuts to Citrix hosts causes users' authentication credentials to be forwarded to the client, which can potentially compromise security.

Secure Endpoint Manager (SEM)

Secure Endpoint Manager is the client application responsible for evalauting EPC, launching agents and bookmarks. Secure Endpoint Manager registers a custom URL sceheme that gets invoked from browser for the specific tasks. SEM has two modules namely, **Web Agent** and **Connect Agent**.

- Web Agent : This unified client is responsible for handling the following:
    - End point control: Performing the end point control checks.
    - Agent installation: Installation and updating connect tunnel.
    - Agent activation: Auto activate OnDemand Proxy and OnDemand Tunnel.
- Connect Agent: This unified client is responsible for handling bookmarks from WorkPlace. This client also provides backward compatibility if someone accesses WorkPlace on prior 12.4 versions.

NOTE: SEM is not displayed as tray icon in the system tool bar.

Topics:

- Supported Operating Systems
- Downloading and Installation
- Installing Secure Endpoint Manager from Client Installation Package
- Setting up the Secure Mobile Access Connect Agent

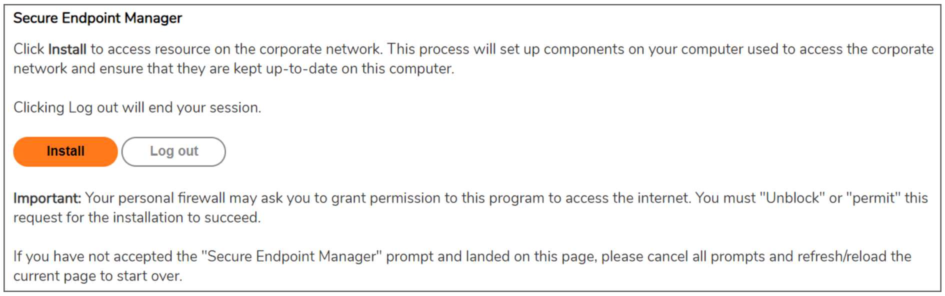
Supported Operating Systems

The Secure Mobile Access Connect Agent currently supports these operating systems:

Operating System	Browser	Version
Windows 11 Windows 10	Edge	Version 96.0 or later
	Chrome	Version 96 or later
	Firefox	Version 95.0 or later
macOS 12.X macOS 11.X macOS 10.15.X	Safari	Version 15.0 or later

Downloading and Installation

On the Welcome page, the install and log out notification displays when you need to launch any native applications:



Secure Endpoint Manager

Click **Install** to access resource on the corporate network. This process will set up components on your computer used to access the corporate network and ensure that they are kept up-to-date on this computer.

Clicking Log out will end your session.

Important: Your personal firewall may ask you to grant permission to this program to access the internet. You must "Unblock" or "permit" this request for the installation to succeed.

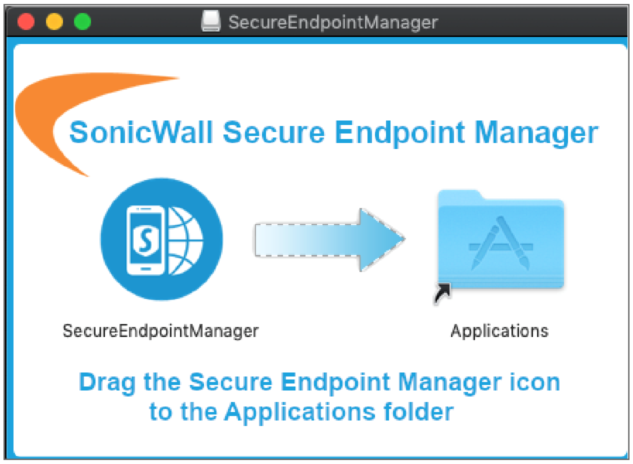
If you have not accepted the "Secure Endpoint Manager" prompt and landed on this page, please cancel all prompts and refresh/reload the current page to start over.

To install the SEM:

1. On the Welcome page, click **Install**.

   Based on your computer operating system, an installer is downloaded.

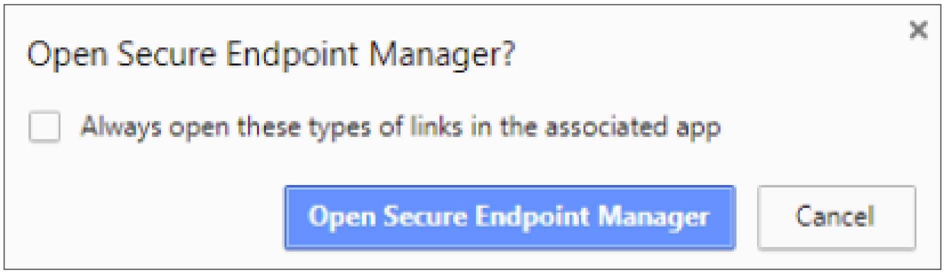
   The Windows installer is `SecureEndPointManager.exe`,and the MacOS installer is `SecureEndPointManager.dmg`. After the download is complete, the Windows installer needs your permission to install and the MacOS installer guides you to copy the Secure Mobile Access Connect Agent in the */Application directory*.

   SecureEndpointManager
SonicWall Secure Endpoint Manager
SecureEndpointManager
Applications
Drag the Secure Endpoint Manager icon to the Applications folder

2. Once the download is complete, run the downloaded installer file.
3. In the confirmation dialog box, click **Run**.
4. On the Welcome page, click **Continue**.

   Based on your web browser, the application could popup a warning message to confirm that you want to launch the Secure Mobile Access Connect Agent. For more information, see Browser Warning.

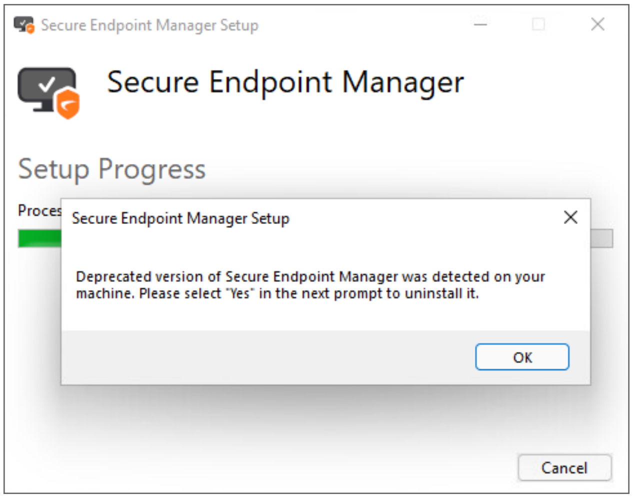


Open Secure Endpoint Manager?

□ Always open these types of links in the associated app

5. Click **Open Secure Endpoint Manager** to launch the Secure Mobile Access Connect Agent.

ⓘ **NOTE:** After successful installation of Secure Endpoint Manager, the unified client checks for deprecated version of agents in the client. If deprecated agents are present a message is displayed to remove the deprecated agents.



Secure Endpoint Manager Setup

Secure Endpoint Manager

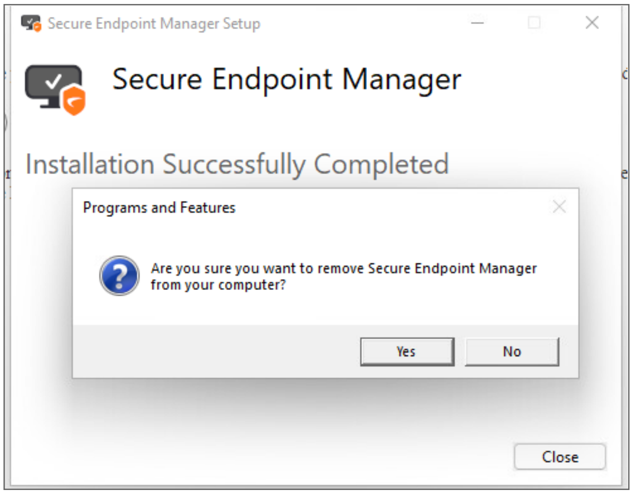
Setup Progress

Proces

Secure Endpoint Manager Setup

Deprecated version of Secure Endpoint Manager was detected on your machine. Please select "Yes" in the next prompt to uninstall it.

- Click **Yes** to remove the deprecated version of SEM.



Secure Endpoint Manager Setup

Secure Endpoint Manager

Installation Successfully Completed

Programs and Features

Are you sure you want to remove Secure Endpoint Manager from your computer?

Installing Secure Endpoint Manager from Client Installation Package

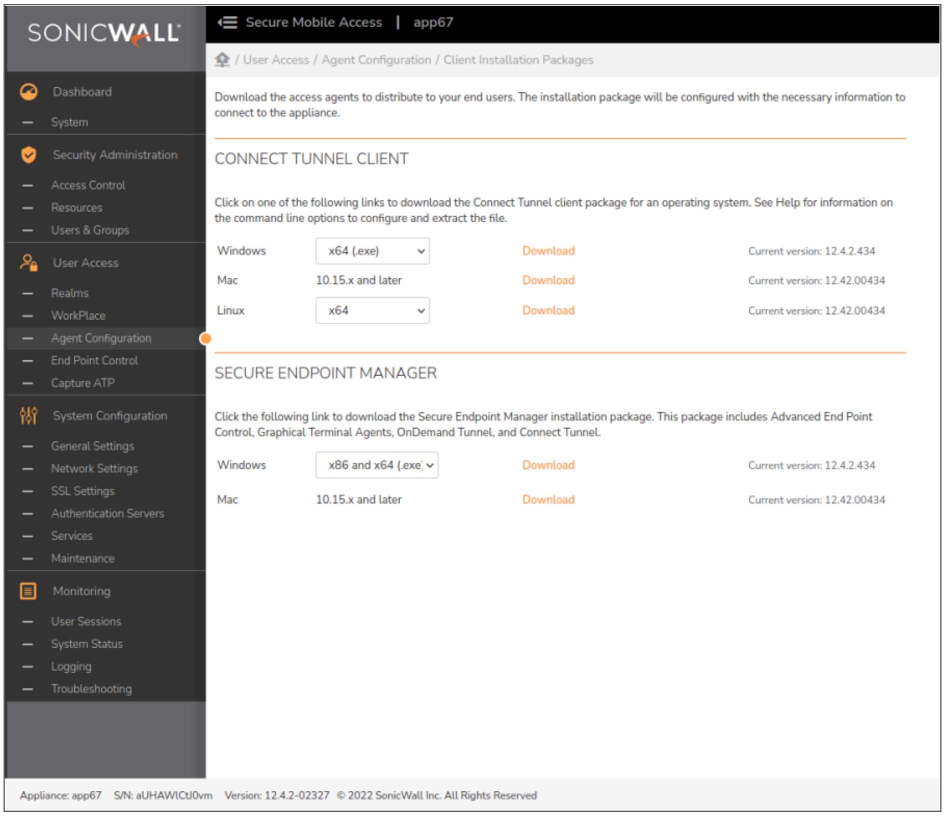
Prerequisits:

- SMA/CMS running 12.4.2 firmware version.

To install SEM from client installation package:

1. In the AMC, navigate to **User Access** > **Agent Configuration**.
2. In the **Access Agents**, next to **Client installation packages**, click **Download**.

   The **Client Installation Packages** page displays.



Download the access agents to distribute to your end users. The installation package will be configured with the necessary information to connect to the appliance.

CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	x64 (.exe)	Download	Current version: 12.4.2.434
Mac	10.15.x and later	Download	Current version: 12.42.00434
Linux	x64	Download	Current version: 12.42.00434

SECURE ENDPOINT MANAGER

Click the following link to download the Secure Endpoint Manager installation package. This package includes Advanced End Point Control, Graphical Terminal Agents, OnDemand Tunnel, and Connect Tunnel.

Windows	x86 and x64 (.exe)	Download	Current version: 12.4.2.434
Mac	10.15.x and later	Download	Current version: 12.42.00434

Appliance: app67 S/N: aUHAWlCtJ0vm Version: 12.4.2-02327 © 2022 SonicWall Inc. All Rights Reserved

3. For **Windows**: In the **Secure Endpoint Manager** click the drop-down next to Windows option and select the installation package based on your operating system and click **Download**.

   ⓘ | **NOTE:** SEM for Windows is supported on platforms such as x86 and x64. The available options are:

   - X86 and X64 (.exe)
   - X86 and X64 (.msi)

   Or

For **Mac**: In the **Secure Endpoint Manager** click **Download** next to Mac option.

The install package is downloaded to your machine.

4. Open the downloaded file and click **Agree** to agree to the terms, then click **Install**.

Setting up the Secure Mobile Access Connect Agent

Topics:

- Proxy Configuration
- Logs
- Exporting logs in SEM
- Browser Warning
- End Point Control
- Personal Device Authorization

Proxy Configuration

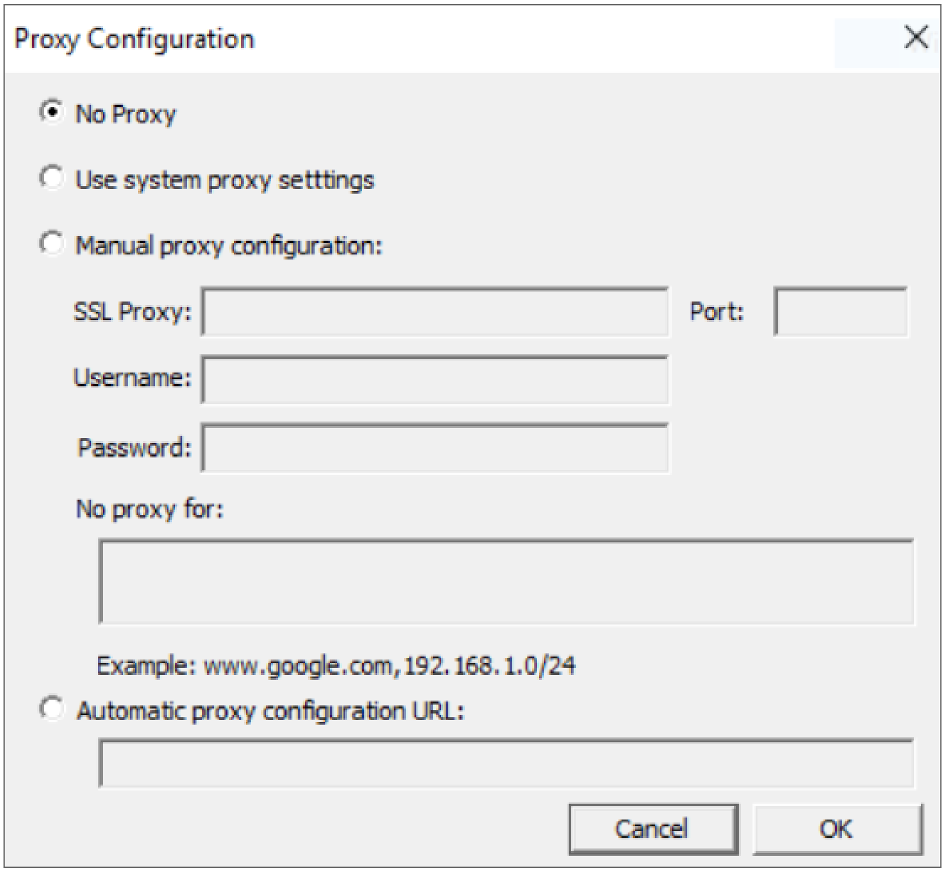
Secure Mobile Access supports proxy deployment, where all client browsers are configured to redirect to a proxy server, but an appliance sits between the client browsers and the proxy server. All Secure Mobile Access features are supported in this scenario, including supporting domain exclusions when the domain is part of a virtual hosting server, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

Additionally, typical data center server farms are fronted with a load balancer and/or reverse SSL Proxy to offload SSL processing on the servers. For a load balancer fronting the servers and doing decryption, the appliance usually only sees the IP of the load balancer, and the load balancer decrypts the content and determines the specific server to assign this connection to. DPI-SSL now has a global policy option to disable an IP-based exclusion cache. The exclusions continue to work even when the IP-based exclusion cache is off. The Secure Mobile Access Connect Agent can setup the proxy by user.

There are four options to setup the proxy configuration:

- **No Proxy** - When no proxy server is configured, IPv6 attributes are discarded.
- **Use system proxy settings**
- **Manual proxy configuration**

- **Automatic proxy configuration URL**



Proxy Configuration

● No Proxy

○ Use system proxy setttings

○ Manual proxy configuration:

SSL Proxy: Port:

Username:

Password:

No proxy for:

Example: www.google.com,192.168.1.0/24

○ Automatic proxy configuration URL:

Logs

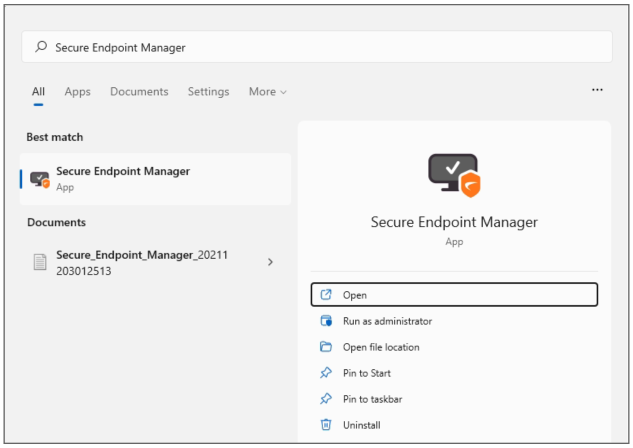
There is a Log tray on the system tool bar. You can right-click the tray and select the popup menu to view the logs.

Exporting logs in SEM

From 12.4.2 onwards, you can clear or export the system logs.

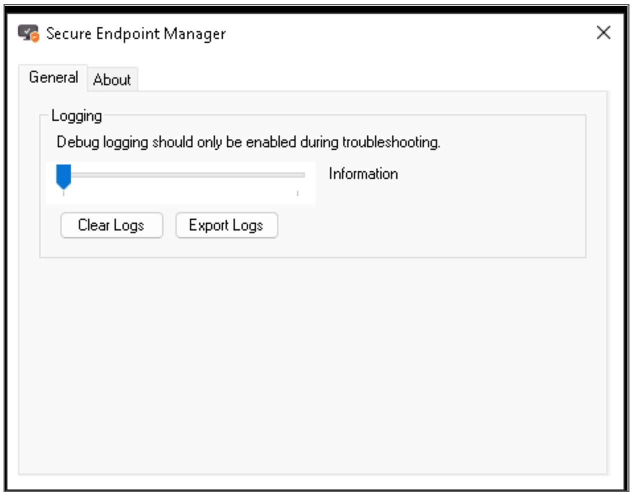
To clear or export logs in SEM:

1. In start menu, select **Secure Endpoint Manager** application.



ⓘ **TIP:** You can go to ***AppData > Local > Programs > SonicWall > Secure Endpoint Manager*** to find the **Secure Endpoint Manager** package.

2. Click **Open**.
3. In **General** Tab, set the log level to either to clear or export the debug logs or information.



Debug logging should only be enabled during troubleshooting.

Information

4. Under **Logging** you can do the following:
   - Click **Clear Logs** to clear the debug logs or information.
   - Click **Export Logs** to export the debug logs or information.

The logs or information files are downloaded.

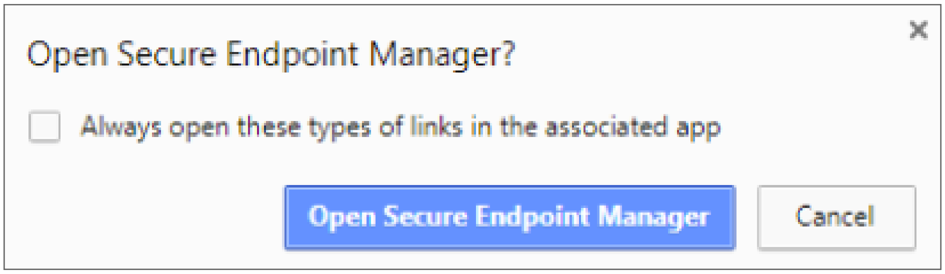
ⓘ **TIP:** You can also go to ***AppData > Local > SonicWall > SnwlWebAgent*** location to collect the logs.

Browser Warning

When the Scheme URL tries to launch the Secure Mobile Access Connect Agent, the browser could popup a warning message to confirm that you want to launch the Secure Mobile Access Connect Agent.

In a Chrome warning window, click **Open Secure Endpoint Manager** to launch the Secure Mobile Access Connect Agent.

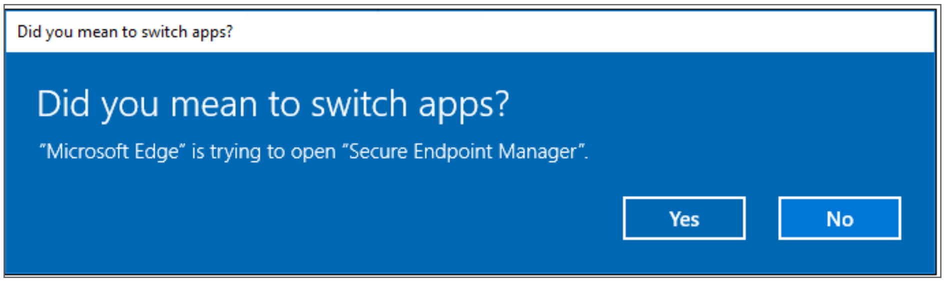
ⓘ **NOTE:** When using Chrome browser in Windows, click **Continue** button to proceed with ODP/ODT activation after EPC checks.



Open Secure Endpoint Manager?

□ Always open these types of links in the associated app

In Microsoft Edge warning window, click **Yes** to launch the Secure Mobile Access Connect Agent.

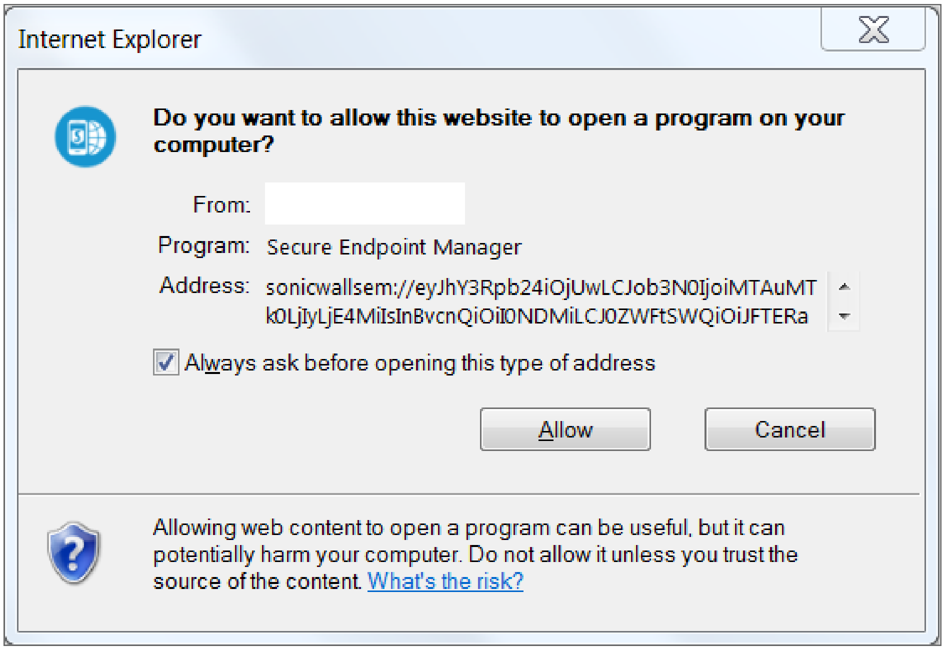


Did you mean to switch apps?

Did you mean to switch apps?

"Microsoft Edge" is trying to open "Secure Endpoint Manager".

In an Internet Explorer warning window, click **Allow** to launch the Secure Mobile Access Connect Agent.



Do you want to allow this website to open a program on your computer?

From:

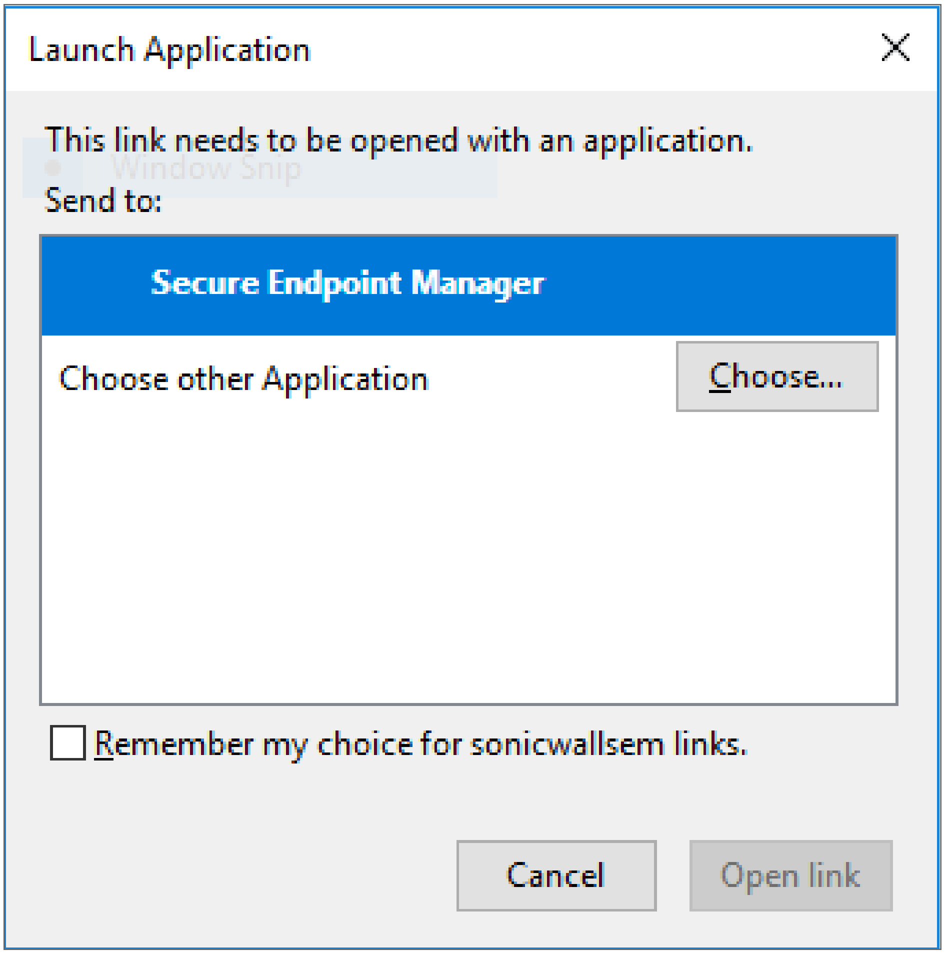
Program: Secure Endpoint Manager

Address: sonicwallsem://eyJhY3Rpb24iOjUwLCJob3N0IjoiMTAuMT
k0LjIyLjE4MiIsInBvcnQiOiI0NDMiLCJ0ZWFtSWQiOiJFTERa

☑ Always ask before opening this type of address

Allowing web content to open a program can be useful, but it can potentially harm your computer. Do not allow it unless you trust the source of the content. What's the risk?

In Firefox warning window, select **Endpoint Manager** and click **Open link** to launch the Secure Mobile Access Connect Agent.



Launch Application

This link needs to be opened with an application.

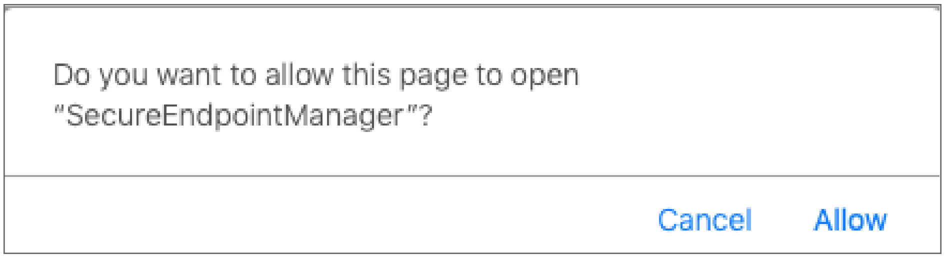
Send to:

Secure Endpoint Manager

Choose other Application

□ Remember my choice for sonicwallsem links.

In Safari warning window, click **Allow** to launch the Secure Mobile Access Connect Agent.



Do you want to allow this page to open "SecureEndpointManager"?

End Point Control

The Secure Mobile Access Connect Agent supports doing an End Point Control (EPC) check from the browser. If you enable the EPC check in the login page, the browser launches the specific Scheme URL requesting the Secure Mobile Access Connect Agent do the EPC check.

The Secure Mobile Access Connect Agent checks the EPC Service on the machine. If the EPC Service is not on the local machine or if there is a newer version on the Appliance, the Secure Mobile Access Connect Agent downloads/Installs or upgrades the EPC Service. After installing or upgrading, the Secure Mobile Access Connect Agent does the EPC check.

Personal Device Authorization

The Secure Mobile Access Connect Agent helps the Personal Device Authorization (PDA) feature get the local machine's information. In the login page, if the user enables the PDA feature, the browser launches the Secure Mobile Access Connect Agent. Secure Mobile Access Connect gets the information of the local machine and sends the information to the appliance.

8

Mobile Connect

Using SMA with Mobile Connect

About using SMA with Mobile Connect

Mobile Connect has general design constraints and implementation issues on iOS, macOS, Android, and ChromeOS. The following information provides considerations and caveats that you may need to know when configuring Mobile Connect to connect to an SMA appliance.

For more information about Mobile Connect, see the Mobile Connect User Guide for your device, available at SonicWall Support.

General Limitations

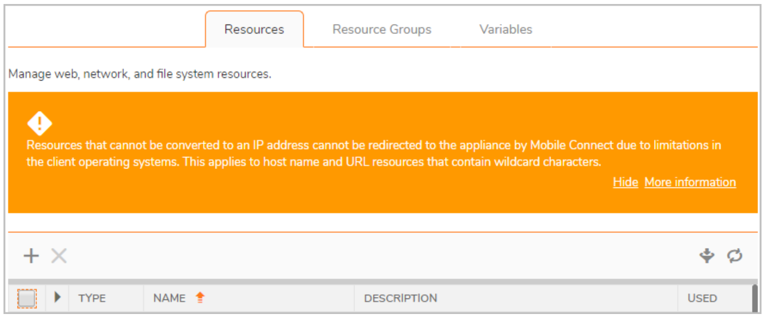
Topics:

- Hostname Redirection
- DNS Routing with Split Tunnel
- DNS Routing with Redirect-All
- File Bookmarks

Hostname Redirection

Mobile Connect on all supported platforms can perform DNS monitoring (like Connect Tunnel for Windows/macOS/Linux), does not have dynamic routing support. If only host name based resource is added, then Mobile Connect will not be able to redirect the traffic for this host resource.:

- To resolve the limitation, all IP subnet or ranges corresponding to a host or domain that the user would access should be added as resources in AMC and included in Access Control rules appropriate for the user/groups that need access to the destination host or domain.
- Because Mobile Connect cannot handle dynamic routing, Secure Mobile Access includes warnings that resources containing wildcards will not work.



Manage web, network, and file system resources.

Resources that cannot be converted to an IP address cannot be redirected to the appliance by Mobile Connect due to limitations in the client operating systems. This applies to host name and URL resources that contain wildcard characters.

DNS Routing with Split Tunnel

In split tunnel, only DNS requests that match the VPN DNS suffix search domains will use the VPN DNS servers. Requests to domains that do not match the VPN DNS suffixes go to the local (3G/WiFi connection) DNS servers. This is true for connections to all server appliances: SMA 1000 series, SMA 100 series, and firewalls. This is a limitation of Apple's iOS.

Example DNS suffix: `example.com`

- Query for `www.example.com` uses VPN DNS Server
- Query for `intranet.corp.example.com` uses VPN DNS Server
- Query for `www.google.com` uses Local DNS server
- Query for `i2.examplecorp.com` uses Local DNS server

This behavior can be overridden in Split Tunnel mode by enabling the **Enable Use tunnel as primary network (Mobile Connect only)** checkbox.

DNS Routing with Redirect-All

In tunnel-all mode (also called Redirect-All), all DNS requests are prioritized to use the VPN DNS servers.

File Bookmarks

File bookmarks allow secure access to files by first checking and enforcing the server configured file policy, and then securely downloading and displaying the file within the Mobile Connect app. Server configured policies include control over whether a file may be printed, copied to the clipboard, opened in a third party app, or securely cached on the iOS device. File bookmarks can also be created to folders or file share root directories to allow directory navigation.

Supported EPC Profiles

End Point Control policy checking is performed before establishing the VPN connection established. Mobile Connect supports the attributes shown in the Supported EPC profiles table.

Attribute	Android	iOS	MacOS	Windows	Linux	ChromeOS
Application	x		x	x	x	x
Client certificate	x	x	x	x	x	x
Directory name	x	x	x	x	x	x
Equipment ID	x	x	x	x	x	x
File name	x	x	x	x	x	x
Android version	x					
iOS version		x				
Antimalware program			x	x	x	
Personal firewall program			x	x	x	
Mac OS version			x			
ChromeOS version						x
Windows domain				x		
Windows registry entry				x		
Windows version				x		
Always on VPN				x		
Linux Kernel version					x	

IPV6 Limitations

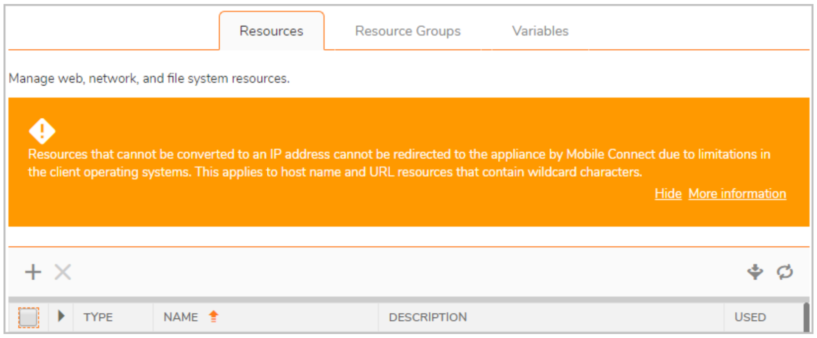
If a device has IPv4 and IPv6 and the DNS host name resolves to an IPv6 record for the appliance, Mobile Connect uses IPv6 to communicate with the appliance. Otherwise, it falls back to IPv4.

URL Control Caveats

The contents of the following fields adversely affect Mobile Connect functions:

- Server field setup with `http` or `https` causes a Mobile Connect failure.
- Realm name limitations require that URLs are correctly formatted, without wild cards in the host name or URL.

Warnings are shown on various page where wild cards might interfere with Mobile Connect operations:



Manage web, network, and file system resources.

Resources that cannot be converted to an IP address cannot be redirected to the appliance by Mobile Connect due to limitations in the client operating systems. This applies to host name and URL resources that contain wildcard characters.

URL Control allows other mobile applications to pass action requests using special URLs to Mobile Connect. These action requests can create VPN connection entries and connect or disconnect VPN connections. For example, another application can launch Mobile Connect, access internal resources as needed, and then disconnect by using the `mobileconnect://` or `sonicwallmobileconnect://` URL scheme. Some common examples of URL Control are:

- Add profile: `mobileconnect://addprofile[/ ]?name=ConnectionName&server=ServerAddress [&Parameter1=Value&Parameter 2 =Value...]`
- Connect: `mobileconnect://connect[/ ]?[name=ConnectionName|server=ServerAddress] [&Parameter1=Value&Paramet er2 =Value...]`
- Disconnect: `mobileconnect://disconnect[/]`

More detailed information is provided in the SonicWall *Mobile Connect User Guide* for your mobile device.

Configuring Trusted Network Detection

The Apple Trusted Network Detection (TND) enhancement to the iOS Connect On Demand feature is available in iOS 6. TND results in the following:

- Can be used only with Connect on Demand.
- Extends the Connect on Demand functionality by determining whether the user is on a trusted network.
- Configured with the iPhone Configuration Utility.
- Used for Wi-Fi connections only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether a VPN should be connected.

Connect On Demand starts a VPN connection whenever a user tries to access a destination with a hostname specified in the domains list. For example, if `*.example.com` is in the **Always Connected** list, when a user accesses `internal.example.com`, the client starts a VPN connection regardless of the network to which the device is currently connected. TND compares the VPN and local DNS servers and DNS suffixes to determine whether to use Mobile Connect and dial the VPN, as shown inthe Trusted Network Detection according to suffixes table.

Trusted Network Detection According To Suffixes

DNS Suffixes	DNS Servers	Login
None	None	Refused - no VPN
None	Same	Refused - no VPN
Same	Same	Refused - no VPN
Same	Same and others	Allowed
Same	Different	Allowed
Different	Same	Allowed
Some	Some	Allowed

Consult documentation from Apple Inc. for more information about Trusted Network Detection and Connect on Demand.

To determine if TND is available for your connection, tap the info indicator in the **Status** row on the **Connection** tab. This displays the buttons used to enable/disable TND if available.

To configure Trusted Network Detection:

1. Tap the **Info** icon in the **Status** row on the **Connection** tab.
2. Ensure **Connect On Demand** is turned on.
3. Turn on **Trusted Networks**.

9

Appendix

- Appliance Command-Line Tools
- Troubleshooting
- Best Practices for Securing the Appliance
- Configuring External SAML Identity Providers
- Log File Output Formats
- Internationalization Support
- SonicWall Support

Appliance Command-Line Tools

- Configuring a New Appliance Using Setup Tool
- Saving and Restoring Configuration Data

Configuring a New Appliance Using Setup Tool

The recommended way to set up a new appliance is to use the LCD controls on the front of the appliance to enter information that will enable a Web browser to connect to your appliance so that you can connect to the Appliance Management Console and run Setup Wizard, as described in Powering Up and Configuring Basic Network Settings.

If you prefer using a command-line utility, you can configure the appliance by running Setup Tool from a serial connection using a laptop computer or terminal.

Topics:

- Tips for Working with Setup Tool
- Using Setup Tool

Tips for Working with Setup Tool

Here are some tips for working with Setup Tool:

- Yes or no questions include a [`y`] or [`n`] at the end of the prompt; type the appropriate letter and then press **Enter** to display the next question.
- To delete a character, press **Backspace**. (On a Windows-based PC, you can also press **Delete** to remove a character.)
- When typing an IP address or netmask, use the standard IP address format of four octets (`w.x.y.z`). Setup Tool provides basic error checking (for example, validating that the gateway you type is on the same subnet as the appliance).
- Type `q` to quit Setup Tool and discard your changes.

Using Setup Tool

When you run Setup Tool from the command line, it prompts you to accept the Secure Mobile Access End User License Agreement (EULA), create a root password, and provide an IP address, subnet mask, and internal default gateway.

To run Setup Tool:

1. Make a serial connection to the appliance (see Powering Up and Configuring Basic Network Settings), and then turn on the appliance using the power button.
2. If the appliance has not yet been configured, or if you have just reset it using either Factory Reset Tool or Config Reset, Setup Tool will run automatically.
3. When you're prompted to log in, type `root` for the username; press **Enter** to move to the next page.
4. You're prompted to type an IP address, subnet mask, and (optionally) a gateway for the internal interface. You use this interface to connect to the appliance from a Web browser and continue setup using AMC.

   `IP address:`

   - Type an IP address for the internal interface connected to your internal (or private) network and then press **Enter**.

   `Subnet mask:`

   - Type a netmask for the internal network interface and then press **Enter**.

   `Gateway:`

   - If the computer from which you'll access AMC is on a different network than the appliance, you must specify a gateway. Type the IP address of the gateway used to route traffic to the appliance and then press **Enter**.

     If you're accessing AMC from the same network on which the appliance is located, simply press **Enter**.
5. You're prompted to review the information you provided. Press **Enter** to accept the current value, or type a new value and then press **Enter**.

6. Finally, you’re prompted to save and apply your changes.
    - Press **Enter** to save your changes.

At this point, Setup Tool saves your changes and restarts the necessary services. It also generates SSL keys using the information you provided (SSH requires security keys that it exchanges with remote SSH clients and servers). After SSH is configured using Setup Tool, it will display a message saying that it is generating these keys.

During this time, you will receive minimal feedback; be patient and do not assume that Setup Tool is not responding. When Setup Tool is finished, a message appears indicating that the initial setup is complete. This message also includes the URL for accessing AMC.

Saving and Restoring Configuration Data

Included on the appliance are a number of command-line administrative tools for saving and restoring configuration data:

- Config Backup Tool—Saves the current configuration file
- Config Restore Tool—Restores a saved configuration file

The AMC method for saving and restoring configuration data is more convenient, but it imports and exports a subset of the data that can be saved and restored using the command-line tools. the AMC method vs. command-line tools table compares the two methods.

AMC Method Vs. Command-line Tools

Configuration item	AMC	Command-line tools
Access policy	x	x
Certificates	x	x
WorkPlace customizations	x	x

Topics:

- Saving Configuration Data

Saving Configuration Data

Backup files are saved to a compressed `aea` file (by default, `/var/backups/cfgback.tgz`). It is a good practice to back up your system regularly, especially when making many system customizations.

To back up your configuration using Backup Tool:

1. Connect to the appliance using SSH or a serial connection, and log in as `root`.
2. Type `config_backup`, specifying any of the following optional parameters:

```
config_backup [-f <tarfile>] [-q] [-d <debuglevel>] [-h]
```

Parameters For Configuration Backup

Parameter	Description
`-f <tarfile>`	Backs up your configuration to the specified file. This parameter is required only if you want to back up to a different backup file than the default file: `/var/backups/cfgback.aea` Setting this parameter is not recommended, because the restore program normally looks for the default file when restoring.
`-q`	Turns off the confirmation prompts (making the backup "quiet"). Normally, you are prompted when you might overwrite an existing backup file.
`-d <debuglevel>`	Specifies how much information to display about the backup operation. Set `<debuglevel>` to an integer between `0` (no information) and `10` (complete information). The default is **1** (normal information).
`-h`	Shows help listing available parameters.

When you run Config Backup Tool, it saves your system configuration files to a backup file with the name and location specified above. If a backup file already exists at that location, you are prompted to confirm that you want to overwrite it (unless you use the `-q` *parameter*).

ⓘ **NOTE:** Your configuration is automatically backed up if you install a new system update using Update Tool. This will not overwrite manual backups created by an administrator.

For additional protection, use a program like SCP to copy the `.tgz` file from the appliance to a separate location, such as a drive on your network or removable media.

You can automate backups by adding Backup Tool to a script. In this case, use the `-q` parameter to suppress confirmation prompts.

Troubleshooting

About Troubleshooting

This Appendix provides general troubleshooting instructions and discusses the troubleshooting tools available in the Appliance Management Console (AMC). Failure in core networking services (such as DHCP, DNS, or WINS) will cause unpredictable failures.

The **User Sessions** page in AMC can be used to monitor, troubleshoot or terminate sessions on your appliance or HA pair of appliances. You can sort through the summary of session details and, if needed, display details on how a device was classified, and why. About 24 hours worth of data is kept; even items that have been deleted or modified are displayed. See Viewing User Access and Policy Details.

General Networking Issues

These troubleshooting tips for networking issues are grouped by type of solution. Before using the ping utility, make sure that **Enable ICMP pings** is enabled on the **Configure Basic Network Settings** page. Some tips are given in these tables:

- the Troubleshooting tips for networking issues table
- the Troubleshooting tips for networking issues: hardware table
- the Troubleshooting tips for networking issues: third-party solutions table

Troubleshooting Tips For Networking Issues

Utility	Troubleshooting tip
Ping the external interface	Ping the external interface to verify the network connection. If you can ping a host's IPv4 or IPv6 address, but not its fully qualified domain name, there is a problem with name resolution. You can issue the `ping` command from the command line or from within AMC (see Ping Command).

Capture network traffic on the external interface	To verify that traffic is reaching the appliance and being returned, use the network traffic utility in AMC, which is based on `tcpdump`. You can send this network traffic data to Technical Support, or review it using a network protocol analyzer like Wireshark. See Capturing Network Traffic for more information.
Ping the network gateway(s)	Ping the external gateway and/or internal gateway. You can issue the `ping` command from the command line or from within AMC. For more information, see Ping Command.
Use ping to test DNS	If you experience DNS problems, first determine whether client DNS resolution is working: 1. Make sure that the client machine has Internet access. 2. At a DOS command prompt, type `ping google.com`. You should see a response like this: `Pinging google.com [nnn.nnn.nnn.nnn]` If basic DNS functionality is available, the IP address in square brackets is resolved by DNS lookup, demonstrating that basic DNS is functioning at the client. If DNS is not available, the ping program will pause for a few seconds and then indicate that it could not find the host `google.com`.
Try to use DNS to resolve the appliance host name	If you continue to experience DNS problems, determine whether DNS can resolve the appliance host name. Repeat the ping procedure described above but replace `google.com` with the host name of your appliance. If `ping` finds: • No address for your host name, troubleshoot the DNS server that should be serving that host name. Try working around client connection issues by replacing the host name with the IP address of the appliance’s external interface. • An address for your host name, but no replies appear (`Request timed out`), ICMP echoes may be blocked at any hop between the client and the appliance.
Clear the ARP	If you’ve recently assigned a new IP address to the appliance, be sure to clear the local Address Resolution Protocol (ARP) cache from network devices such as firewalls or routers. This ensures that these network devices are not using an old IP-to-MAC address mapping.

Troubleshooting Tips For Networking Issues: Hardware

Hardware	Troubleshooting tip
Cables	Check all network cables to be sure you don't have a bad cable.

Bypass the firewall	If you're using network address translation (NAT), you might be blocked by a firewall. Temporarily bypass the firewall by connecting a laptop to the appliance on the physical interface using a cable, and then verify network connectivity. If this type of connection is impractical, try placing your laptop on the same network segment as the external interface of the appliance (to get as close to the appliance as possible).
Configure the switch port	If you experience network latency, such as slow SCP file copying or slow performance by the Web proxy or network tunnel service, the problem may be due to configuration differences between the appliance interface settings and the switch ports to which the appliance is connected. It’s possible for a switch to improperly detect duplex-mode settings (for example, the appliance is configured at full duplex but the switch detects half duplex). Cisco has documented such problems with its switches. To resolve this problem, disable auto negotiation. Instead, configure the switch port to statically assign settings that match the appliance. You must check both switch ports and both appliance interface settings (internal and external, if applicable). If even one interface/switch port is mismatched, performance suffers. If you are experiencing network latency but your appliance/switch ports are configured correctly, the problem lies somewhere else in the network. It could also be an application-level issue (such as slow name resolution on the DNS server being accessed by the Web proxy or network tunnel service).

Troubleshooting Tips For Networking Issues: Third-party Solutions

Third-party solution	Troubleshooting tip
Verify that traffic is not being filtered out	Review the contents of the log file */var/log/kern.iptables* while a connection attempt is failing. If packets are reaching the appliance but are being dropped or denied by **iptables** (a firewall running on the appliance), review the **iptables** ruleset by running the following command: `iptables -L -n -v` Traffic that is filtered by **iptables** is logged but not forwarded to an external syslog server.

Verify a Downloaded Upgrade File

You can use AMC to install version upgrades, as described in Upgrading, Rolling Back, or Resetting the System. To make sure that the update was successfully transferred to your local computer, compare its checksum against the one in the `.md5` file you extracted from the `.zip` file.

To verify the MD5 checksum on your PC, use a Windows- or Java-based utility. Microsoft, for example, offers an unsupported command line utility on their site named File Checksum Integrity Verifier (FCIV):

To verify the downloaded file on a PC:

1. At the DOS command prompt, type the following, which returns a checksum for the downloaded file:

   ```
   fciv <upgrade_filename>.bin
   ```

2. Open the associated `.md5` file (which you downloaded from the MySonicWall Web site) using Notepad or another text editor:

   ```
   notepad <upgrade_filename>.bin.md5
   ```

3. Compare the two check sums. If they match, you can safely continue with your update. If they differ, try the download again and compare the resulting check sums. If they still don't match, contact SonicWall Technical Support.

To verify the downloaded file on the appliance:

1. Type the following command, which returns a checksum for the downloaded file:

   ```
   md5sum <upgrade_filename>.bin
   ```

2. Open the associated `.md5` file:

   ```
   cat <upgrade_filename>.md5
   ```

3. Compare the two checksums.

AMC Issues

One of the most common errors in AMC is to make a configuration change and then forget to apply it. A **Pending changes** link appears in the top-right corner in AMC whenever changes have been made but not applied. Click the link, and then click **Apply Changes** to automatically restart the services.

Troubleshooting AMC Issues

Issue	Solution
Can't access AMC	If you can't access AMC, connect a cable to the internal network interface on the appliance and verify that you can access AMC without any network. If this type of connection is impractical, put the laptop on the same network segment as the internal interface (to get as close to the appliance as possible). If you still can't access AMC, make sure your URL includes the `https://` protocol identifier. Also verify that you've included the port number 8443 in the URL.
Can’t log in to AMC on the internal network	If your browser cannot log in to AMC on the internal network, ensure that traffic from the client to the IP address of the appliance’s internal interface actually arrives at the internal interface. Using the network traffic utility in AMC, which is based on `tcpdump`, you can capture traffic on the internal interface (`eth0`). Any client attempts to reach AMC should show traffic TCP SYN packets from the client’s IP address directed to port 8443. See Capturing Network Traffic for more information.

Can’t log in	If AMC login fails with the error `Invalid Login Credentials`, verify the spelling of your username and password. Passwords are case-sensitive; ensure that **Caps Lock** and **Num Lock** are not enabled.
CPU utilization is spiking	If you are using nested group lookup on your LDAP or AD authentication server, make sure that you are also caching the lookup results: searching the entire directory tree takes time and increases the CPU usage on both the appliance and your authentication server.

Authentication Issues

An authentication server is referenced in a realm.

Troubleshooting Authentication Issues

Issue	Solution
Access to the external authentication server(s)	Verify that you can access the external authentication server by using the network traffic utility in AMC, which is based on `tcpdump`. You can send this network traffic data to Technical Support, or review it using a network protocol analyzer like Wireshark. See Capturing Network Traffic for more information.
Authentication server credentials	Verify that AMC contains the proper credentials for access to your external server. For LDAP, check the **Login DN** and **Password** settings, and click **Test Connection**. For RADIUS, check the **Shared secret** setting.
Authentication server logs	Review the authentication server logs. Make sure you're not entering invalid credentials or having connectivity problems.
User authentication using an LDAP or AD server takes too long or times out	If you are using nested group lookup on your LDAP or AD server, make sure that you are also caching the lookup results, because searching the entire directory tree takes time. To reduce the load on your directory and get better performance, cache the attribute group or static group search results by selecting the **Cache group checking** checkbox.

Using Personal Firewalls with Agents

Some firewall products display a security alert during the provisioning of Secure Mobile Access agents or EPC components. This is because the firewalls are regulating outbound connections by process (in addition to port and protocol). In most cases, the user can simply “unblock” or “permit” the outbound connection.

Connect Tunnel users should configure their personal firewalls to allow the Secure Mobile Access VPN service (`ngvpnmgr.exe`) and Secure Endpoint Manager (`AventailComponents.exe`) to access the Internet and to add the SMA appliance by host name or IP address as a trusted host or zone.

There are a few firewalls, such as one supplied by Trend Micro, that do not permit a user with restricted rights to override the firewall settings. For corporate systems on which users have limited access rights, you may need to update the firewall settings before deploying the Secure Mobile Access VPN so that users won't have to respond to security prompts.

Consult the documentation for your corporate personal firewall to determine the firewall policy. If a firewall update proves necessary, a rule that allows all processes to communicate with the appliance over port 443 is recommended.

Secure Mobile Access Services Issues

To see a brief summary of which services are running, click Services on the main navigation menu.

Topics:

- Web Proxy Service Issues
- Tunnel Issues

Web Proxy Service Issues

- Temporarily increase the server log level in AMC to **Verbose**. (Don't forget to click **Pending changes** in the top-right corner of any AMC page, and then click **Apply Changes** to automatically restart the service.)
- To see the Web proxy service log, click **Logging** in the main navigation menu, and then select **Web proxy audit log** from the **Log file** list. Verify that your connection request appears in the log.
- Verify that your DNS server can resolve the Web proxy service **Server name** setting in AMC to the IP address of the Web proxy service interface. You can use the lookup tool within AMC (see Using DNS Lookup), or you can issue the `nslookup` or `dig` commands from a command prompt.
- If your network uses NAT to translate IP addresses, make sure that the Web proxy service **Server name** setting contains the IP address of the outside (or public) IP address that is being substituted using NAT.

Tunnel Issues

This section describes how to troubleshoot problems with the network tunnel service and the tunnel clients.

Topics:

- Installation
- Connectivity

See also:

- Windows Client Troubleshooting
- MacOS and Linux Tunnel Client Troubleshooting

Installation

Troubleshooting Installation Issues

Issue	Troubleshooting tips
Connect Tunnel client does not install	The provisioned client is delivered to client computers as an installation package. If the installation procedure fails, the following may explain the issue or offer a solution: • System is not supported: Ensure that the client computer’s system software is supported by the Connect Tunnel client. • Client software doesn’t match system requirements: If users can access WorkPlace, install the client that is available in WorkPlace. • User does not have local administrator rights: Users must have administrator rights to install the Connect Tunnel client. • The Connect Tunnel client installation log file (`ngsetup.log`) may contain information that can help troubleshoot installation issues. On Windows Vista, the file is located in the `ProgramData` folder, which is hidden by default: `[drive:]\ProgramData\SMA1000\ngsetup.log`

OnDemand Tunnel agent does not install	The OnDemand Tunnel client is automatically installed and activated when a user browses to WorkPlace after authenticating in an appropriately configured realm. Typically, the OnDemand Tunnel agent operates without user intervention, providing secure, tunneled access to configured resources as long as WorkPlace is running. If the OnDemand Tunnel agent fails to install or activate, the following may explain the issue or offer a solution: • Installing OnDemand Tunnel requires administrator rights. • OnDemand Tunnel not enabled for this Workplace realm: On the main navigation menu in AMC, click **Realms**. The **Realms** page displays a list of all realms defined for the appliance. To review the settings affecting the network tunnel service for a particular realm, click the realm name. On the **Communities** tab of the **Configure Realm** page, click **Edit** in the **Access Methods** area. Ensure that the **Network tunnel client** checkbox is selected. • System is not supported: Ensure that the client computer's system software is supported by the OnDemand Tunnel agent. • Browser is not supported: Ensure that the user is running a Web browser that is supported by the OnDemand Tunnel agent. See Client Components for system requirements.

Connectivity

Troubleshooting Connectivity Issues

Issue	Troubleshooting tips

Client does not connect	The OnDemand Tunnel agent starts automatically after users successfully authenticate to WorkPlace, if the community supports the OnDemand Tunnel agent. The provisioned Connect Tunnel client requires you to activate it each time you want to begin a tunnel session. Tunnel sessions can remain active for many hours. Interrupting network connectivity for periods of more than a few seconds causes the tunnel session to end. Interruptions occur, for example, when a network cable is disconnected, a laptop is set to sleep, or the network link is so busy that it has high latencies and packet drop rates. The following describes common failures that can prevent a Connect Tunnel client or OnDemand Tunnel agent connection from succeeding: • Appliance is unreachable: In the Connect Tunnel login box, click **Properties**. In the **Properties** box, under **Login group**, click **Change**. If the appliance is reachable over the network, the **Select** or **enter your login** box will be populated with a list of available realms. If the appliance is not reachable, after a few moments you will see an error message that reads "The remote network connection has timed out." • Incorrect appliance address specified: In the Connect login box, click **Properties**. In the **Properties** box, ensure that the **Host name or IP address of your VPN** is correct. If a host name is entered instead of an IP address, ensure that the client can resolve the host name, and that the host name corresponds to the IP address of the appliance's external interface. • Appliance is not running: Ensure that the appliance is running. • Invalid realm for user name: Ensure that a valid realm is configured for the user. • Authentication failure: Ensure that the user has specified the correct authentication credentials. • Client service failure: Retrieve the client log (`ngsetup.log`), and send the log file to SonicWall for analysis along with a description of the situation. • Personal firewall is not permitting tunnel traffic: Ensure that the user's firewall is configured to allow connections to the appliance's FQDN or IP address.

Client connects, but cannot access a resource	When a tunnel is established, an icon representing that tunnel appears in the taskbar notification area. At this point the client computer has access to all configured resources the appliance can reach and for which the user is authorized. If the client cannot reach a resource, the following may explain the issue or offer a solution: • Resource not defined: Ensure that the correct resource is defined in AMC. • User not authorized to access resource: In AMC, review access control rules, and realm and community assignments, to ensure that the user is allowed to access the resource. • Appliance routing cannot reach resource: Ensure that there isn’t a general networking problem between the appliance and back-end resources. • Server software failure: Note the time of the failure, determine whether the network tunnel service is functioning properly, and gather further troubleshooting information if necessary.

Client connects, but disconnects unexpectedly	Once connected, a Connect Tunnel or OnDemand Tunnel connection should remain active for many hours. However, the tunnel can end prematurely for several reasons. If a tunnel connection disconnects unexpectedly, the following may explain the issue or offer a solution: • Tunnel that was left idle timed out: To conserve appliance resources, idle tunnels can disconnect after an extended period of time. • Administrator stopped or restarted the network tunnel service: Normal configuration operations using AMC should not affect established tunnels; they continue to operate under the configuration that was in effect when they were established. However, configuration changes that affect basic appliance networking will cause existing tunnels to drop or hang, possibly requiring a disconnect at the client to recover. • With the network tunnel service logs set to Info level or higher, the message, `Reset Internal Interface and Addressing Information`, appears in the log any time the network tunnel service is stopped; in addition, the message, `Internal Interface eth0 Address` *n.n.n.n* `Netmask` *n.n.n.n* `BCastAddr` *n.n.n.n* `Subnet` *n.n.n.n* (with appropriate IP addressing values), appears any time the service is started from a stopped condition. In the `ngutil` log, the text, `The server is shutting down`, identifies this situation. • Internetwork carrying tunnel became unresponsive or unreliable: When traffic fills the available bandwidth on any hop between the client and the appliance, packets wait on queues in the end-point TCP stack or in intermediate routers. When queues fill, packets are dropped. • The network tunnel service carries traffic over a TCP SSL connection. TCP is designed to accept network unreliability by delivering traffic only when it is in sequence, it can be verified, and it is available. TCP implementations can drop connections when ACK responses are not returned soon enough; this is true of the Windows TCP implementation. After the connection drops, the tunnel client’s normal behavior is to attempt to resume the connection transparently for 20 seconds. If congestion caused the drop, resumption is likely to fail, and the user sees the tunnel terminate. • Cluster failover occurred, and client’s resumption failed: In a cluster configuration, when an active node fails over to the standby node, client connections are preserved by the client tunnel resumption mechanism. Clients will continue tunnel resumption attempts for 20 seconds, and then give up; if the failover is not complete within this time the tunnel connection is dropped. On orderly termination the client does not attempt resumption, so all tunnel connections are dropped. • In addition, a new client connection initiated after failover, but during the period in which tunnel clients are attempting resumption, might be assigned an address that an existing client is trying to resume using. Several characteristics of address assignment make this case unlikely, but if it occurs the resuming client’s tunnel is dropped.

Client connects, but disconnects unexpectedly (continued)	• Client service failure: Failure of the client service software can cause the tunnel to drop, and an error box to appear. Retrieve the client log, send the log file to SonicWall for analysis along with a description of the situation, and then restart the service. • Server software failure: Failure of the appliance tunnel software generally causes a spontaneous reboot of the appliance, or possibly an indefinite hang. • In the reboot case, a crash dump appears in a numbered directory in `/var/log/dump`; retrieve and analyze this information. • If the appliance hangs without rebooting, the crash dump may have succeeded before the hang; reboot the appliance and check `/var/log/dump` for a new crash dump, and then retrieve and analyze this information. You may need to reproduce the circumstances that led to the crash.
General server problems	Tunnel problems typically show up at the client first. Many possible problems can be identified only by an administrator in AMC or, sometimes, at an SSH console or the system serial console. For more information, see General Networking Issues.

Network tunnel service is not running	At the serial console or in an SSH session, type: `uscat /var/avt/vpn/status` If the network tunnel service is configured and running, client virtual address range information will appear. Otherwise, nothing will appear except another shell prompt. The following items can help you determine why the network tunnel service is not running. • License invalid or expired: If your appliance license is invalid, AMC displays a license warning at the top- right corner of every AMC page after login. You may need to contact SonicWall to resolve licensing issues. • Stopped in AMC or from console prompt: In the **Network Tunnel Service** area of the AMC **Services** page, you can stop the network tunnel service indefinitely, and you can view information that indicates whether the service has been stopped. • Service unconfigured, or incorrectly configured: The network tunnel service must be configured with virtual addresses and related information for assignment to clients. If tunnel service configuration is incomplete, the service will not run. • Server software failure: A failure of a userspace network tunnel service component will generally cause the failed component to restart. There may be helpful information in the log or in a corefile in `/var/log/core`. Serious failure of a kernel component will likely result in a crash dump. • Cluster issues: Clustered appliances must be able to communicate over their cluster interfaces. If they cannot communicate reliably, both nodes in the pair may attempt to provide service, resulting in failures, or both nodes may be on standby, so that neither is providing service.

Client Troubleshooting

This section provides client troubleshooting information for Windows, Mac, and Linux clients.

Topics:

- Windows Client Troubleshooting
- MacOS and Linux Tunnel Client Troubleshooting

Windows Client Troubleshooting

If you want to remove the Secure Mobile Access software components, follow these steps:

- Resetting Browser
- Uninstalling Secure Mobile Access Components

- Logging Back In to WorkPlace

Resetting Browser

Follow these steps to reset browser and Java settings. Where applicable, the instructions for Internet Explorer, Google Chrome, and Firefox Mozilla are given:

- Clear Cookies and Cache
- Reset Security Zones to Defaults
- Reset Advanced Settings to Defaults
- Reset Privacy Settings to Defaults

Clear Cookies and Cache

To clear browser cookies and cache in Internet Explorer:

1. Click **Tools > Internet Options**.
2. Click **Delete Files** and **Delete Cookies**.

To clear browser cookies and cache in Mozilla Firefox:

1. Click **Tools > Clear Private Data.**
2. Select at least these three checkboxes:
   - **Cookies**
   - **Cache**
   - **Authenticated Sessions**
3. Click **Clear Private Data Now**.

To clear browser cookies and cache in Google Chrome:

1. Click **Tools > Clear browsing data**.
2. Select at least these checkboxes:
   - **Delete cookies and other site and plug-in data**
   - **Empty the cache**
3. Click **Clear browsing data.**

Reset Security Zones to Defaults

To reset the security level for all Web content zones in Internet Explorer:

1. Click **Tools > Internet Options > Security** tab.
2. Highlight a Web content zone (for example, **Internet**), and then click the **Default Level** button. Do this for each zone.

Reset Advanced Settings to Defaults

To reset advanced Internet Explorer settings:

1. Click **Tools > Internet Options > Advanced** tab.
2. Click the **Restore Defaults** button.

Reset Privacy Settings to Defaults

To reset Internet Explorer privacy settings:

1. Click **Tools > Internet Options > Privacy** tab.
2. Click the **Default** button.

Uninstalling Secure Mobile Access Components

To uninstall all Secure Mobile Access files:

1. Reboot your computer. This ensures that no files are loaded in memory and makes the uninstall easier.
2. Remove all Secure Mobile Access components:
    a. In the **Control Panel**, open **Add/Remove Programs**.
    b. Remove each Secure Mobile Access component.
3. Reboot the computer.

Logging Back In to WorkPlace

Log back in to WorkPlace, install Secure Endpoint Manager, and let the Secure Mobile Access components load.

If something goes wrong during client or agent installation, the error is recorded in a client installation log. This log is automatically uploaded to the appliance and listed in AMC if Secure Endpoint Manager is installed. Users who do not have Access Manager are prompted to upload the log file to the appliance when an installation error occurs.

MacOS and Linux Tunnel Client Troubleshooting

When troubleshooting MacOS and Linux tunnel client problems, request the system and version information described in this section from your users. Before gathering this information, users should uninstall and re-install the software.

Topics:

- MacOS System and Application Information
- Linux System and Application Information

MacOS System and Application Information

Have users specify the information listed in the MacOS system and application information table.

MacOS System And Application Information

System information	How to find it
Operating system	Select **About this Mac** from the Apple menu.
`hostfino` command	Open the Terminal application (in the Applications > Utilities folder) and type hostfino. This displays processor and kernel information, along with the amount of available memory.
Safari browser	Select **About Safari** from the Safari menu.
System Profiler	1. Select **About this Mac** from the Apple menu. 2. Click **More Info** to open the **System Profiler**. The profiler displays detailed information about the computer's hardware and installed software. The complete report (if you choose to print it) can easily be over 100 pages long.

When you start Connect Tunnel, make sure that debug mode is enabled. Slide to enable **Enable Debug Logging** and on the **General** tab click **Clear Logs**or **Export Logs** buttons.

Linux System and Application Information

Have your users enable debug logging and clear the current set of logs before attempting to reproduce an issue. Once the issue is reproduced, export the logs to SonicWall Support.

Use the **Enable Debug Logging** checkbox, **Clear Logs** button, and **Export Logs** button on the **General** tab to perform these functions:

Troubleshooting Tools in AMC

You can monitor, troubleshoot or terminate sessions on your appliance, filtering them by user name, realm (authentication server), community, access agent, traffic load, and so on—and then get a quick summary of particular sessions. Several basic network tools are also available, including ping, traceroute, DNS lookup, a routing table viewer, and a way to capture and filter network traces for backend connectivity troubleshooting.

Topics:

Using DNS Lookup

You can use AMC's Lookup tool to determine how DNS is resolving an IP address or a host name. This tool is useful for troubleshooting various DNS problems (for example, it can determine whether your DNS server is running).

Use a fully qualified domain name or an IP address to specify a host in the Lookup tool. However, you can type a non-qualified host name as long as you have defined one or more default search domains on the **Configure Name Resolution** page (available from the **Network Settings** page in AMC). For details on name resolution, see Configuring Name Resolution.

To determine how DNS is resolving an IP address or host name:

1. In the AMC, navigate to **Monitoring > Troubleshooting**.
2. Click the **Lookup** tab.
3. In the **Address** field, type the IP address or host name of the machine against which you want to issue the command.
4. Click **Go**.

Viewing the Current Routing Table

You can view the current routing table from within AMC.

To view the current routing table:

1. In the AMC, navigate to **Monitoring > Troubleshooting**.
2. Click the **Routes** tab.
3. Click **Go**. The routing table is displayed.

Capturing Network Traffic

This network traffic utility, which is based on tcpdump, allows you to capture a packet-by-packet list of the data going in and out of the appliance. If you are new to troubleshooting, you can use this utility to generate a file of network traffic data that can be sent to Technical Support for troubleshooting network issues. If you are familiar with troubleshooting and reading trace files, you can analyze the traffic using a network protocol analyzer, such as Wireshark.

Capturing all network traffic on your appliance can quickly result in files that are too unwieldy to analyze. Where possible, use filters to restrict the traffic to issues you are troubleshooting.

Packet captures are saved on the appliance with a filename created from the date or time that the capture was performed. From 12.4.2 onwards, the description field is used to generate a filename. When the captures are downloaded from the appliance and sent to the support has a description to the filename, which makes it easy to understand.

ⓘ | **NOTE:**

- If description of the capture contain non alpha-numeric chars, it is replaced with underscore.

  For example, if the file name has a description like *Internal&External* then filename would be App220_20220121_143802IST_Internal_External.zip.
- If more than one capture contains same description, file names will be differentiated with the capture date and time.
- If two different captures contain same description downloaded from two different appliances, capture filename will always start with appliance name to differentiate between them.
- Only 30 characters are allowed for a filename. If the description is long, it is truncated.

The following sample procedure demonstrates how to filter by host and port (in this example, an Exchange server and Web traffic).

To filter and capture network traffic to a file on the appliance:

1. From the main navigation menu under **Monitoring**, click **Troubleshooting**.
2. Click the **Network Traffic** tab.
3. To restrict the capture to traffic coming from or going to your Exchange server, enter the server's full qualified domain name or IPv4 or IPv6 address in the **These hosts** field. For example, `exchange.mycompany.com`.
4. To make sure that you are capturing only the HTTP traffic, select `Web (HTTP or HTTP/S)` from the **Common ports** list; only traffic to and from the HTTP and HTTPS ports (80, 443, 8080, and 8443) will be captured.
5. Click **Start** to begin capturing traffic. Enter a user-friendly filename or description.

   The size limit for a single capture is 500 MB of raw data; when the size of a capture file reaches 100 MB, it "rolls over" into a separate file (large files are difficult to process with packet analysis tools such as Wireshark). If the total size of a single capture reaches 500 MB (five files of 100 MB each), the capture automatically stops. During a capture, the **Size** column indicates how close you are to the limit.

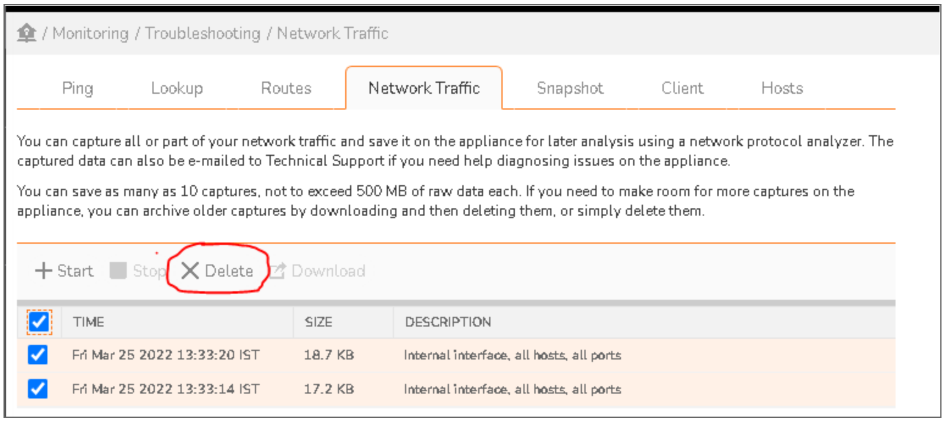
6. Click **Stop** to stop capturing traffic.

   The capture file is a `.zip` file that is stored on the appliance and listed here. (The figure in the **Size** column indicates how much room the file is using on the appliance; this is the size of the compressed `.zip` file, not the raw data.) The maximum number of files you can store is ten; as more capture files are added, the oldest ones are dropped from the list.

   A description added in the filename is displayed.

   Multiple captures can be created and stored in appliance. Observe that stored captures are displayed in a table view with checkbox for multiple selection.

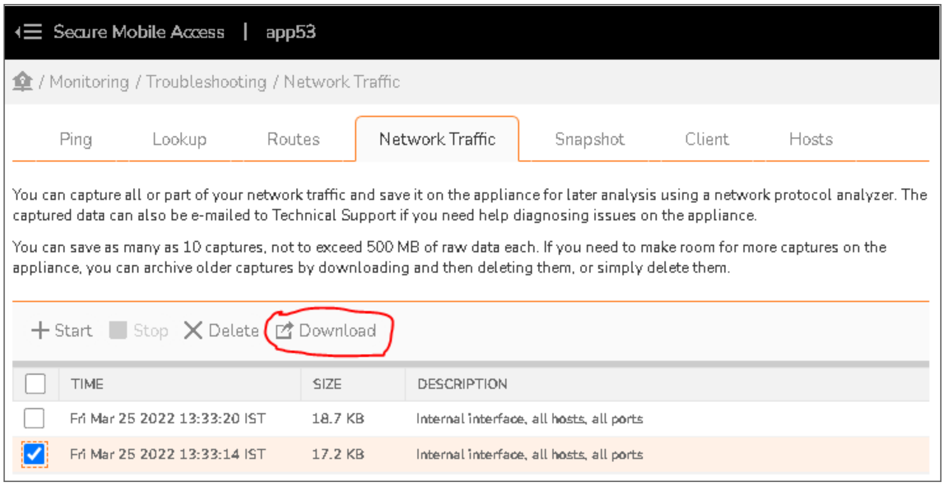
   ⓘ **NOTE:** When multiple captures are selected, the **Delete** option is enabled. When a single capture is selected, both the **Download** and the **Delete** options are enabled.



You can capture all or part of your network traffic and save it on the appliance for later analysis using a network protocol analyzer. The captured data can also be e-mailed to Technical Support if you need help diagnosing issues on the appliance.

You can save as many as 10 captures, not to exceed 500 MB of raw data each. If you need to make room for more captures on the appliance, you can archive older captures by downloading and then deleting them, or simply delete them.

☑	TIME	SIZE	DESCRIPTION
☑	Fri Mar 25 2022 13:33:20 IST	18.7 KB	Internal interface, all hosts, all ports
☑	Fri Mar 25 2022 13:33:14 IST	17.2 KB	Internal interface, all hosts, all ports



You can capture all or part of your network traffic and save it on the appliance for later analysis using a network protocol analyzer. The captured data can also be e-mailed to Technical Support if you need help diagnosing issues on the appliance.

You can save as many as 10 captures, not to exceed 500 MB of raw data each. If you need to make room for more captures on the appliance, you can archive older captures by downloading and then deleting them, or simply delete them.

□	TIME	SIZE	DESCRIPTION
□	Fri Mar 25 2022 13:33:20 IST	18.7 KB	Internal interface, all hosts, all ports
☑	Fri Mar 25 2022 13:33:14 IST	17.2 KB	Internal interface, all hosts, all ports

   ⓘ **NOTE:** The limit for stored capture is 10 and not exceed 500 MB of size. The older captures can be deleted or downloaded.

7. To download captured data, click the button corresponding to the file you want to analyze or send to Technical Support, and then click **Download**. Each capture file is a `.zip` file containing the captured network traffic (for example, `eth0.cap`) and a `readme` text file outlining what filters were used, if any, and when the data was captured.

```
Comment: Internal interface, hosts: exchange.mycompany.com, selected ports
```

```
Internal interface (eth0): enabled
External interface (eth1): disabled
Protocol: <All>
Hosts: exchange.mycompany.com
Ports: 80,443, 8080, 8443
Start time: Wed Aug 15 2007 17:56:52 GMT
Stop time: Wed Aug 15 2007 17:58:31 GMT
```

> **NOTE:** Captured network traffic is not encrypted and may contain passwords and other sensitive information. If you have security concerns about storing a downloaded capture or sending it over an unsecured Internet connection, use Snapshot Tool in AMC instead. You can make a partial snapshot that includes only network captures, and then choose to encrypt the results. See Snapshot Tool for more information.

You can capture network traffic on either of the appliances in a high-availability pair (the master node or the slave node).

Logging Tools for Network Tunnel Clients

To capture a session during which a user is running either of the network tunnel clients, have users follow these steps and email you the results. The Windows procedure differs from the one for MacOS and Linux users.

To run ngutil on a Windows client computer:

1. Go to a command prompt: Click **Start > Run**, and then type `cmd` in the **Open** field; if you are using Windows Vista, Click **Start**, and then type `cmd` in the **Start Search** field.
2. At the command prompt, clear the event log and set the severity level by typing the following command:

   ```
   ngutil -reset -severity=debug
   ```
3. Start the network tunnel client and perform any actions the system administrator wants captured in the log.
4. At the command prompt, type `ngutil > log.txt` to write the buffered log messages to a file named `log.txt` in the current directory.
5. Send the `log.txt` file to the administrator.
6. Alternatively, you can run `ngutil -poll` to see real-time logging on the client computer. (Press **Ctrl-C** to stop logging.)

> **NOTE:** You can also have users type the `ngutil -tail=1000>client-log.txt` command; this sends the most recent 1000 lines in the client log to a file named `client-log.txt` in plain text.

For more information on the syntax for the `ngutil` command, type `ngutil -help` at the command prompt.

To save session information on a client computer (MacOS or Linux):

1. Start the network tunnel client and perform any actions the system administrator wants captured in the log.
2. On the client device, locate the files `AvConnect.log` and `AvConnectUI.log` and send them to the administrator.

Using CEM Extensions

SonicWall Technical Support may ask you to use Secure Mobile Access Configuration Extension Mechanism (CEM) advanced URL extensions. These CEM extensions are used to access advanced AMC pages and should only be used when instructed to do so by Technical Support.

Contact SonicWall Support at https://support.sonicwall.com/.

CEM Advanced Features

The Configuration Extension Mechanism (CEM) is a generic mechanism to allow simple configuration to be done for features that appear in maintenance releases or hotfixes. The CEM page allows the configuration of arbitrary key-value pairs for enabling advanced functionality. These key-value pairs are read from the extension config file by each service that has a patch generated for it (custom drop, hotfix, or maintenance release).

Advanced features should be used only under SonicWall Support supervision. Contact SonicWall Support for additional instructions.

Ping Command

Use the `ping` command to verify a network connection. When you issue the `ping` command, it sends an ICMP ECHO_REQUEST packet to a target host and waits to see if the host answers.

To issue a ping command:

1. In the AMC, navigate to **Monitoring > Troubleshooting**.
2. Click the **Ping** tab.
3. In the **Address** field on the **Ping** page, type the IPv4 or IPv6 address or host name of the machine you want to ping.
4. Click **Go**. AMC issues the ping command.

   After about five seconds, the results should appear in the large box at the bottom of the page. If the ping command cannot reach the host, it returns results resembling the following:

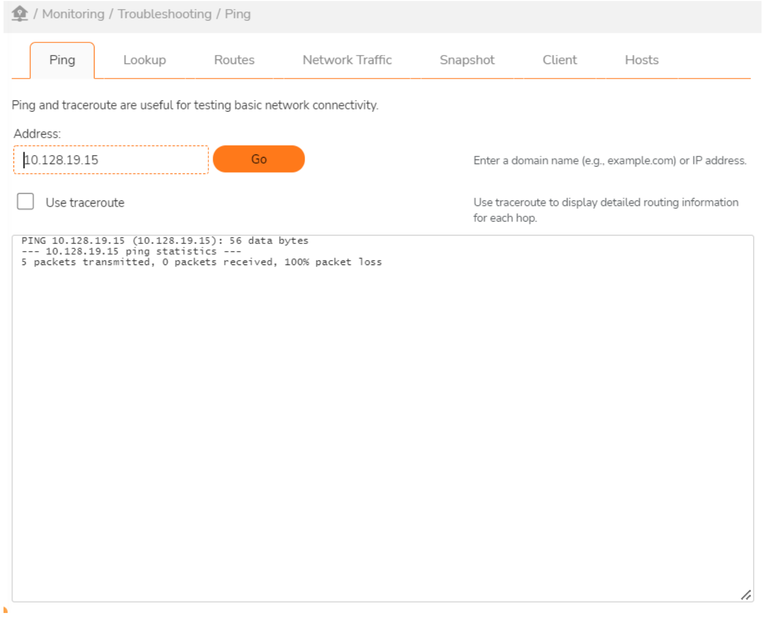
   ```
   PING 10.128.19.15 (10.128.19.15): 56 data bytes

   --- 10.128.19.15 ping statistics ---

   5 packets transmitted, 0 packets received, 100% packet loss
   ```

Traceroute Command

Use the traceroute command to see the sequence of gateways through which an IP packet travels to reach its destination. This can help you find a network failure point.

To issue a traceroute:

1. In the AMC, navigate to **Monitoring > Troubleshooting**.
2. Click the **Ping** tab.
3. In the **Address** field, type the IP address or host name of the machine against which you want to issue the `traceroute` command.
4. Select the **Use traceroute** checkbox.
5. Click **Go**. The **Traceroute** returns a list of hosts, starting with the first gateway and ending with the destination.



Ping and traceroute are useful for testing basic network connectivity.

Address: 10.128.19.15

Enter a domain name (e.g., example.com) or IP address.

□ Use traceroute

Use traceroute to display detailed routing information for each hop.

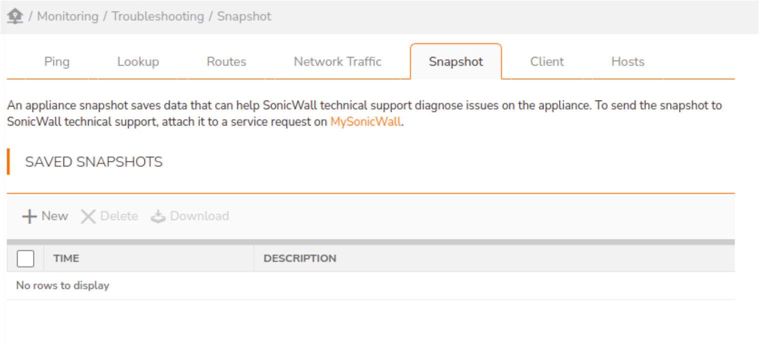
```
PING 10.128.19.15 (10.128.19.15): 56 data bytes
--- 10.128.19.15 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Snapshot Tool

A snapshot of your configuration can help SonicWall Technical Support or other IT professionals diagnose any problems you are having with the appliance. This file, especially if it includes core dump files, can be quite large (the File Download in the final step will tell you how large).

To save, delete, restore and download a snapshot:

1. In the AMC, navigate to **Monitoring > Troubleshooting**.
2. Click the **Snapshot** tab.



/ Monitoring / Troubleshooting / Snapshot

Ping | Lookup | Routes | Network Traffic | Snapshot | Client | Hosts

An appliance snapshot saves data that can help SonicWall technical support diagnose issues on the appliance. To send the snapshot to SonicWall technical support, attach it to a service request on MySonicWall.

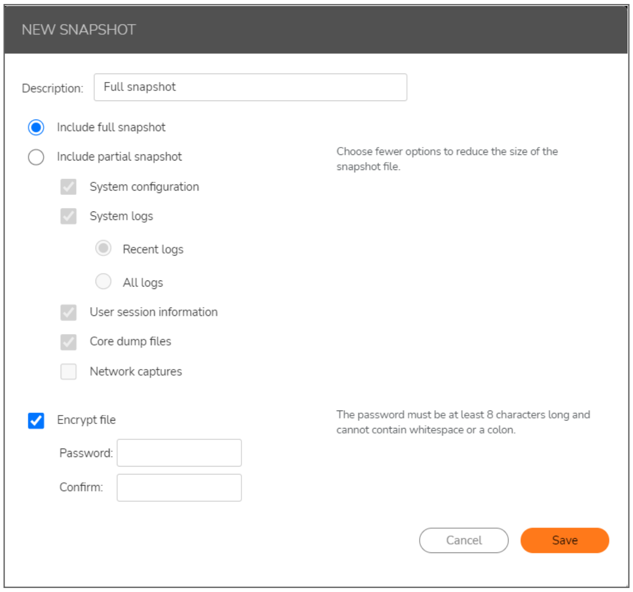
SAVED SNAPSHOTS

+ New ✕ Delete Download

□	TIME	DESCRIPTION

No rows to display

3. Click **New** to create snapshot
4. Select **Include full snapshot** or **Include partial snapshot**.



NEW SNAPSHOT

Description: Full snapshot

● Include full snapshot

○ Include partial snapshot

Choose fewer options to reduce the size of the snapshot file.

☑ System configuration

☑ System logs

● Recent logs

○ All logs

☑ User session information

☑ Core dump files

□ Network captures

☑ Encrypt file

The password must be at least 8 characters long and cannot contain whitespace or a colon.

Password:

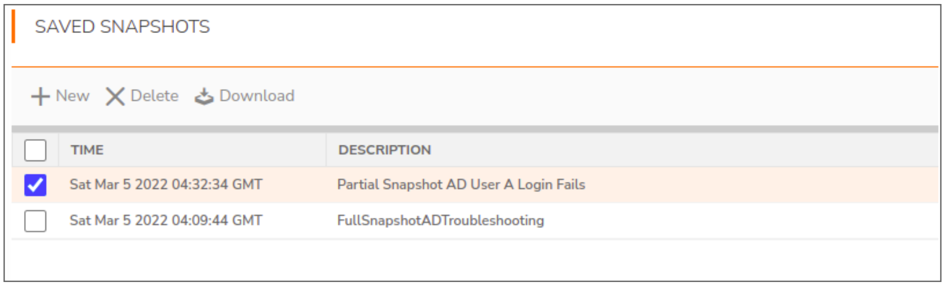
Confirm:

Cancel Save

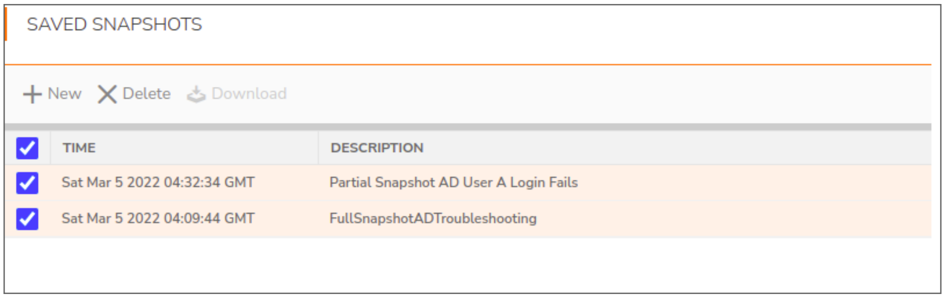
5. If you select **Include partial snapshot** then you can select the following information to be included:
   - **System configuration**
   - **System logs**
     - **Recent ones** or **All logs**.
   - **User session infomration**
   - **Core dump files**
   - **Network captures**
6. If you plan to send the file to SonicWall Technical Support, you should select **Encrypt file** to keep sensitive information secure. Technical Support will need the password you assigned to this archive so that they can decrypt the file. Make sure you send it in such a way that it meets your internal security requirements (over the phone or by secure email, for example).
7. Click **Save snapshot.** The files are saved in a zip archive named `snapshot.tgz`.

Multiple snapshots can be created and saved in appliance. Observe that saved snapshots are displayed in a table view with checkbox for multiple selection.

ⓘ **NOTE:** When multiple snapshots are selected, the **Delete** option is enabled. When a single snapshot is selected, both the **Download** and the **Delete** options are enabled.



□	TIME	DESCRIPTION
☑	Sat Mar 5 2022 04:32:34 GMT	Partial Snapshot AD User A Login Fails
□	Sat Mar 5 2022 04:09:44 GMT	FullSnapshotADTroubleshooting



☑	TIME	DESCRIPTION
☑	Sat Mar 5 2022 04:32:34 GMT	Partial Snapshot AD User A Login Fails
☑	Sat Mar 5 2022 04:09:44 GMT	FullSnapshotADTroubleshooting

ⓘ **NOTE:** The limit for saved snapshots is 10. The older snapshots are deleted automatically when more than 10 snapshots are created.

8. Click the **Download** to save the compressed file locally.

Host Connectivity Testing

From 12.4.2 onwards, you can test all the resource hosts or URLs for connectivity. This feature helps to secure the system and verifies the backend configured host certificates.

The following servers and resource hosts are tested.

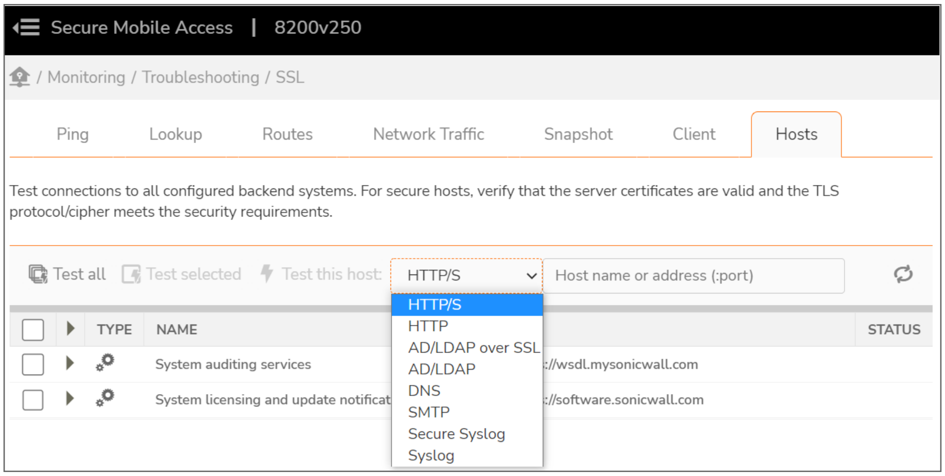
- SonicWall systems:
  - geows.global.sonicwall.com and lm2.sonicwall.com (CMS only)
  - software.sonicwall.com
  - wsdl.sonicwall.com

    ⓘ **NOTE:** software.sonicwall.com and wsdl.sonicwall.com are available by default for testing.
- NTP servers
- Intune back end:
  - login.microsoftonline.com
  - graph.microsoft.com (when intune enabled)

- URL resources (both https and http).
- Serverfarm resources.
- Host resources (verify DNS names are resolvable in configured DNS)
- Authentication Servers:
    - AD basic/LDAP (primary/secondary servers)
    - AD advanced (KDC and GC DNS entries)
    - Radius/Defender UNPW (verify hostnames resolve)
    - Radius/Defender Token (verify hostnames resolve)
    - LDAP Certificate
    - AD/LDAP/ADTree over SSL
- SMS Service Providers.
- SMTP Server.
- Syslog Server(s)

To test configured hosts:

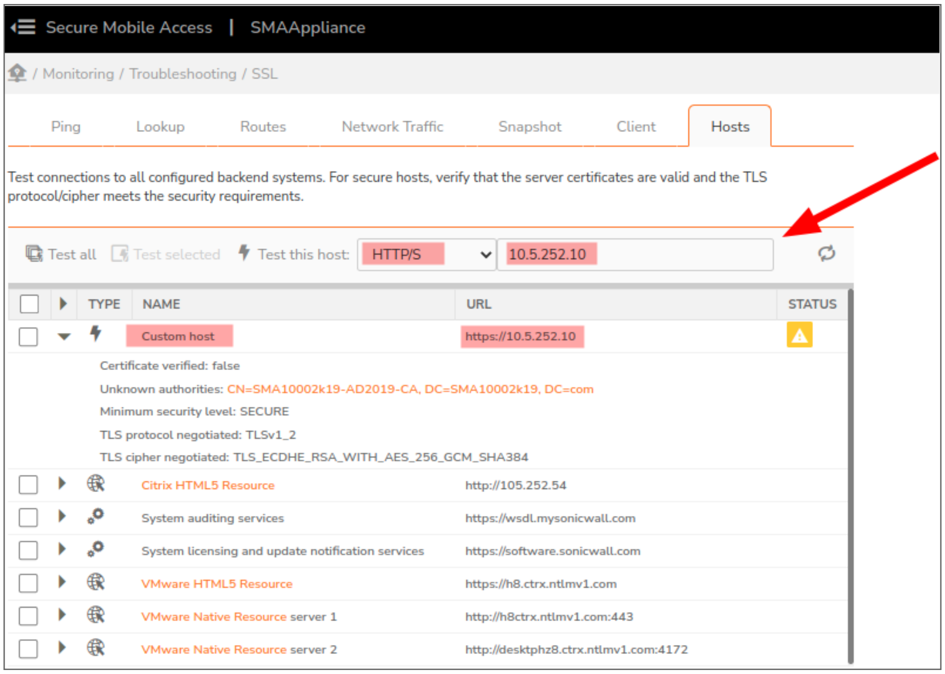
1. In the AMC, navigate to **Monitoring** > **Troubleshooting**.
2. Click the **Host** tab.
   All the configured resource or host urls are displayed.



Test connections to all configured backend systems. For secure hosts, verify that the server certificates are valid and the TLS protocol/cipher meets the security requirements.

	TYPE	NAME		STATUS
□		System auditing services	://wsdl.mysonicwall.com	
□		System licensing and update notificat	://software.sonicwall.com	

3. To test all the resources, click **Test all**.
   Or
   To test required resource, select the required host (already configured in AMC) checkbox and click **Test selected**.
   Or
   To test custom resource, which is not configured in AMC, select the type of protocol and enter the URL to test and click **Test this Host**.


Secure Mobile Access | SMAAppliance
/ Monitoring / Troubleshooting / SSL
Ping
Lookup
Routes
Network Traffic
Snapshot
Client
Hosts

Test connections to all configured backend systems. For secure hosts, verify that the server certificates are valid and the TLS protocol/cipher meets the security requirements.

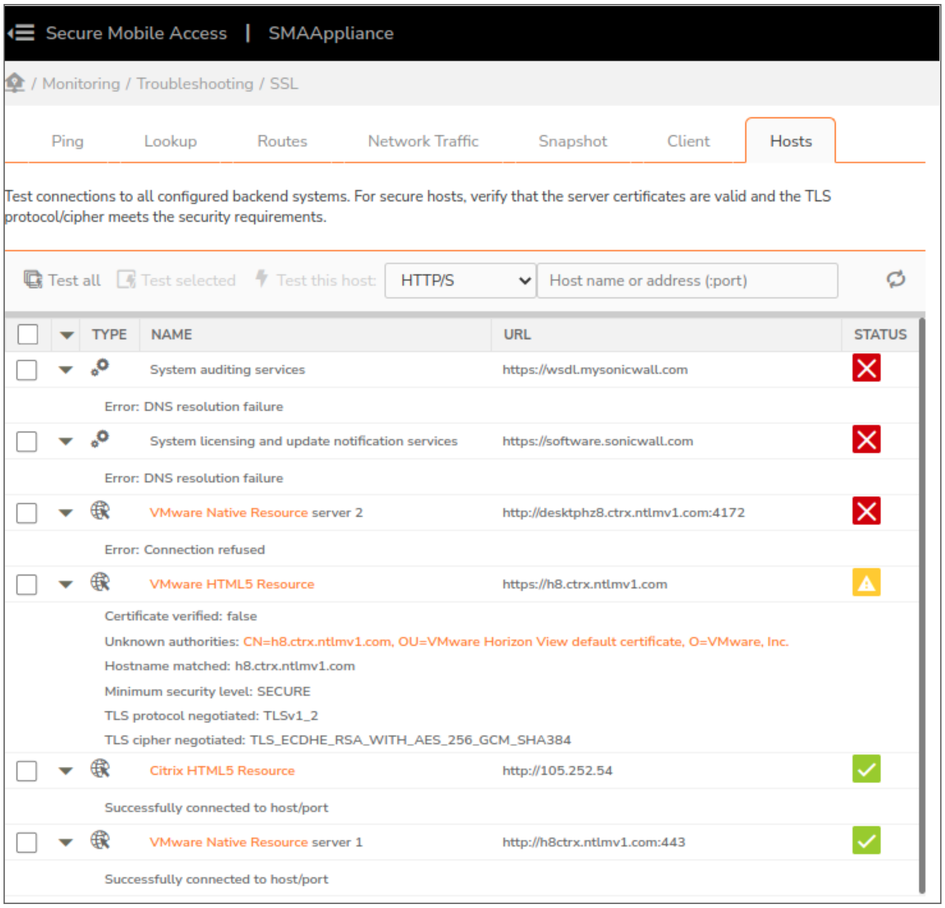
Test this host: HTTP/S 10.5.252.10

□	▸	TYPE	NAME	URL	STATUS
□	▾	⚡	Custom host	https://10.5.252.10	⚠
□	▸		Citrix HTML5 Resource	http://105.252.54	
□	▸		System auditing services	https://wsdl.mysonicwall.com	
□	▸		System licensing and update notification services	https://software.sonicwall.com	
□	▸		VMware HTML5 Resource	https://h8.ctrx.ntlmv1.com	
□	▸		VMware Native Resource server 1	http://h8ctrx.ntlmv1.com:443	
□	▸		VMware Native Resource server 2	http://desktphz8.ctrx.ntlmv1.com:4172	

Expanded details for Custom host:

Certificate verified: false
Unknown authorities: CN=SMA10002k19-AD2019-CA, DC=SMA10002k19, DC=com
Minimum security level: SECURE
TLS protocol negotiated: TLSv1_2
TLS cipher negotiated: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The successful and failed tests results are displayed under **Status**.



Secure Mobile Access | SMAAppliance

/ Monitoring / Troubleshooting / SSL

Ping | Lookup | Routes | Network Traffic | Snapshot | Client | **Hosts**

Test connections to all configured backend systems. For secure hosts, verify that the server certificates are valid and the TLS protocol/cipher meets the security requirements.

Test all | Test selected | Test this host: HTTP/S | Host name or address (:port)

	TYPE	NAME	URL	STATUS
□		System auditing services	https://wsdl.mysonicwall.com	☒
		Error: DNS resolution failure		
□		System licensing and update notification services	https://software.sonicwall.com	☒
		Error: DNS resolution failure		
□		VMware Native Resource server 2	http://desktphz8.ctrx.ntlmv1.com:4172	☒
		Error: Connection refused		
□		VMware HTML5 Resource	https://h8.ctrx.ntlmv1.com	⚠
		Certificate verified: false Unknown authorities: CN=h8.ctrx.ntlmv1.com, OU=VMware Horizon View default certificate, O=VMware, Inc. Hostname matched: h8.ctrx.ntlmv1.com Minimum security level: SECURE TLS protocol negotiated: TLSv1_2 TLS cipher negotiated: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		
□		Citrix HTML5 Resource	http://105.252.54	✓
		Successfully connected to host/port		
□		VMware Native Resource server 1	http://h8ctrx.ntlmv1.com:443	✓
		Successfully connected to host/port		

4. For the failed tests, click on the resource and expend to see the error for failure.

Best Practices for Securing the Appliance

- Network Configuration
- Appliance Configuration
- Appliance Sessions
- Administrator Accounts
- Access Policy
- Set Up Zones of Trust
- Setting security level
- Client Access

Network Configuration

You can configure most of the settings in the following list of best practices on the **Network Settings** and **Services** pages in AMC:

- Configure the Appliance to Use Dual Interfaces
- Configure the Appliance to Use Dual Network Gateways
- Protect both Appliance Interfaces with Firewalls
- Enable Strict IP Address Restrictions for the SSH Service
- Enable Strict IP Address Restrictions for the SNMP Service
- Use a Secure Passphrase for the SNMP Community String
- Disable or Suppress ICMP Traffic
- Use an NTP Server
- Protect the Server Certificate that the Appliance is Configured to Use

Configure the Appliance to Use Dual Interfaces

The appliance optimizes firewall settings when it is configured with both an external and internal interface. Services are split between the interfaces so that management services, such as the AMC, listen only internally. Public services, such as the Secure Mobile Access access services, listen only externally.

Configure the Appliance to Use Dual Network Gateways

Dual network gateways allow you to leverage your existing network routers, which means less overhead for the appliance administrator, and provide a more manageable network configuration as your network grows and evolves.

Protect both Appliance Interfaces with Firewalls

- Allow traffic from the Internet only on ports 80, 443, and 4500.
- Give the appliance access to only the necessary resources on the customer network.
- Allow only trusted IP addresses from the customer network to access AMC.

Enable Strict IP Address Restrictions for the SSH Service

If both network interfaces are enabled, Secure Shell (SSH) listens on both interfaces. Be sure to restrict SSH service access to the IP addresses of trusted management workstations or, at a minimum, the address range of the internal network.

Enable Strict IP Address Restrictions for the SNMP Service

If both network interfaces are enabled, Simple Network Management Protocol (SNMP) listens on both interfaces. Restrict SNMP service access to the IP addresses of trusted management workstations or, at a minimum, the address range of the internal network.

Use a Secure Passphrase for the SNMP Community String

By default, the SNMP configuration in AMC sets the string your network management tool uses to query the SMA appliance in the **Community string** field to **public**. Be sure to change this to a secure passphrase.

Disable or Suppress ICMP Traffic

If both network interfaces are enabled, enabling Internet Control Message Protocol (ICMP) makes it possible for someone to discover the appliance from the Internet. The most secure approach is to disable ICMP or enable ICMP only on the internal interface. If you do enable ICMP , you should suppress ICMP Echo Request traffic using a firewall or other network device.

Use an NTP Server

Synchronize with an external Network Time Protocol (NTP) server to ensure accurate timestamps in the system logs, and to ensure that time-based security checks—such as password and certificate expiration—occur properly.

Protect the Server Certificate that the Appliance is Configured to Use

Don’t leave the appliance server certificate where others can access it, and always make sure the key is encrypted with a strong password. If attackers obtain it, it will tell them which host it is associated with and will enable them to decrypt private data.

Appliance Configuration

You can configure most of the settings in the following list of best practices on the **Maintenance** page in AMC.

Keep the software image on the appliance updated

Use the **Update** page to apply hotfixes and upgrade files promptly because they often contain security fixes.

Make regular configuration backups

Periodically back up your current configuration using one of these methods in AMC:

- The **Export** option on the **Import/Export** page; see Exporting the Current Configuration to a Local Machine.
- If you prefer, you can save the backup to your appliance; see Saving the Current Configuration on the Appliance.

Appliance Sessions

Your AMC session automatically times out after 15 minutes of inactivity (the length of the timeout period is not configurable). To end an AMC session, click **Log out** in the top-right corner of AMC. (If you terminate a session by closing your Web browser instead, the session is listed as logged in until it times out 15 minutes later.)

When **Auto-refresh** is set to any time interval other than *Off* while one of these pages is displayed, the refresh activity prevents the AMC session from automatically timing out after 15 minutes. This means that if you leave AMC unattended while one of these pages is displayed and in auto-refresh mode, AMC will not time out. A good security practice is to switch to another page in AMC when you are done viewing system status or logs.

Administrator Accounts

To configure administrator accounts, click **General Settings** in the main AMC navigation menu, and then click **Edit** in the **Administrators** area.

Use a Strong Password

Your password should be at least eight characters long and should contain punctuation characters, a combination of uppercase and lowercase letters, and numbers.

Change the AMC Administrator Password

The AMC administrator password is set to the same value as the root password during the initial installation. It is good practice to change the AMC administrator password because it is transmitted in an SSL tunnel between the Web browser and the AMC server. If the password for the primary administrator (whose username is `admin`) is changed, the password for logging in to the appliance directly (as `root`) is also changed.

Change Administrator Passwords often and don’t Share Them

It is good practice not to share passwords with anyone unless necessary. If you need to enable access for other administrators, create individual administrative accounts. One person should own the administrator account, and the password should be kept in escrow or some other safe place.

Limit the Number of Administrative Accounts and Assign Administrative Privileges only to Trusted Individuals

Restrict the access of secondary administrators. AMC's role-based administration enables the primary administrator to grant limited administrative control to secondary AMC administrators. For more information, see Defining Administrator Roles.

Access Policy

To create, edit, or reorder access rules, click **Access Control** in the main AMC navigation menu. Use the following guidelines when you create rules:

- Follow the Principle of "Least Privilege"
- Pay Close Attention to Rule Order
- Put your Most Specific Rules at the Top of the List
- Carefully Audit Rules Containing "Any"

Follow the Principle of "Least Privilege"

The most secure approach to policy design is to specifically list the resources to which you want to permit access. Anything not accounted for in the "permit" rules is denied by the appliance. This approach follows one of the fundamental design principles of computer security: that access rights should be explicitly required, rather than given to users by default.

An alternate approach is to create "deny" rules for restricted resources, but permit access to everything else by default. Here, anything not accounted for in the "deny" rules is accessible, until the final "deny" rule is processed. This method may be easier to set up, but is more error-prone and thus not as secure.

Of course, you can also use a combination of permit and deny rules. In this case, users are permitted access to some resources, but denied access to others.

Pay Close Attention to Rule Order

Because the appliance processes your access control rules sequentially, the order in which you organize them has great significance in terms of whether access is permitted or denied. The appliance stops reading the rules as soon as it finds a match. Carefully review your security policy settings to avoid inadvertently placing rules in the wrong order.

Put your Most Specific Rules at the Top of the List

Putting broader rules that grant more permissions at the top of the list may cause the appliance to find a match before it has a chance to process your more restrictive rules. As a general rule, it is best to put your most specific rules at the top of the list.

Carefully Audit Rules Containing “Any”

If you create a rule that does not restrict access to a particular user or destination resource, the word “any” appears in the access control list.

Carefully consider the impact of “any” in your policy rules. For a “permit” rule, too many criteria that apply to “any” could expose a security hole. On the other hand, too many “deny” rules for “any” could unnecessarily restrict network access.

Set Up Zones of Trust

You can define “zones of trust” that provide different levels of access depending on the level of trust at the user’s end point. Connection requests are compared against device profiles you set up in AMC and are then assigned to the appropriate zone. See About End Point Control for more information.

To set up zones of trust:

1. Set up a **Deny** zone. Deny zones are evaluated first. If there is a device profile match (for example, a certain file or registry key is found on the device), the user is denied access and logged out. See Creating a Deny Zone for more information.
2. Set up a **Quarantine** zone. A device for which there is no profile match is placed in the quarantine zone (if one has been defined). You can customize the message users see; for example, you may want to explain why the user is quarantined and what is required to bring the user’s system into compliance with your security policies. See Creating a Quarantine Zone for more information.

Setting security level

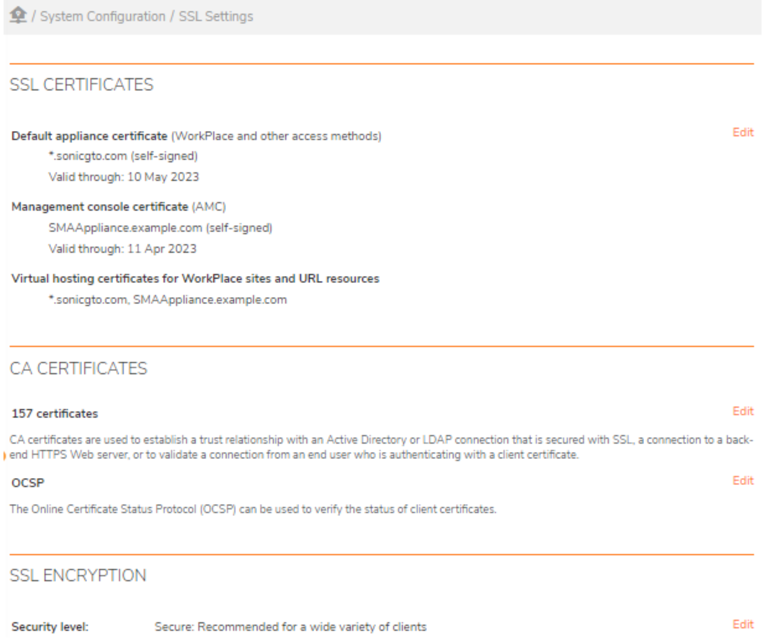
When you configure the protocols and compression settings for encrypting traffic, you can set security level.

The AMC, WorkPlace, Workplace, and Tunnel will all conform to the SSL protocols that are enabled on the **Configure SSL Encryption** page to enforce protocols and ciphers on connecting clients.

The AMC logs SSL connection failures if the client/browser fails to negotiate an SSL connection due to incompatible ciphers or protocols. These messages are logged at the ERROR level to help the administrator troubleshoot SSL compatibility problems.

To set security level you want:

1. Navigate to **System Configuration > SSL Settings**.



/ System Configuration / SSL Settings

SSL CERTIFICATES

Default appliance certificate (WorkPlace and other access methods) Edit

*.sonicgto.com (self-signed)

Valid through: 10 May 2023

Management console certificate (AMC)

SMAAppliance.example.com (self-signed)

Valid through: 11 Apr 2023

Virtual hosting certificates for WorkPlace sites and URL resources

*.sonicgto.com, SMAAppliance.example.com

CA CERTIFICATES

157 certificates Edit

CA certificates are used to establish a trust relationship with an Active Directory or LDAP connection that is secured with SSL, a connection to a back-end HTTPS Web server, or to validate a connection from an end user who is authenticating with a client certificate.

OCSP Edit

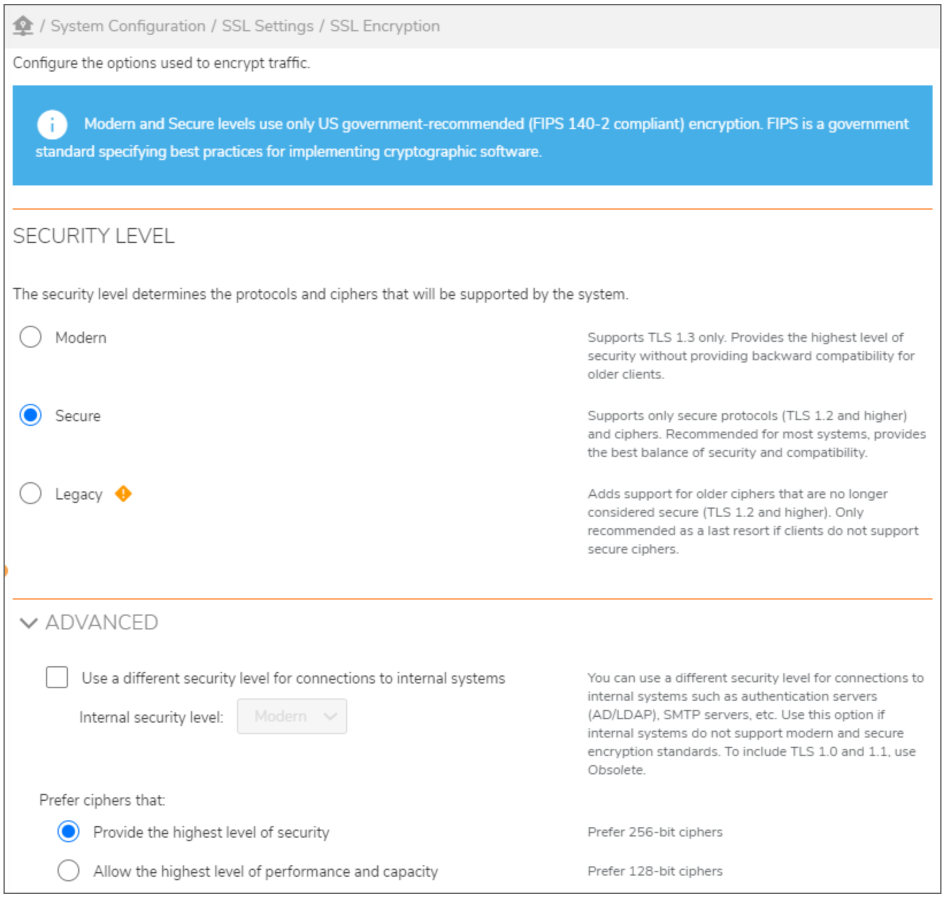
The Online Certificate Status Protocol (OCSP) can be used to verify the status of client certificates.

SSL ENCRYPTION

Security level: Secure: Recommended for a wide variety of clients Edit

ⓘ | **NOTE:** A warning will appear when you have a less secure protocol or cipher enabled.

2. In the **SSL Encryption** section, click **Edit**. The **SSL Encryption** page displays.



/ System Configuration / SSL Settings / SSL Encryption

Configure the options used to encrypt traffic.

Modern and Secure levels use only US government-recommended (FIPS 140-2 compliant) encryption. FIPS is a government standard specifying best practices for implementing cryptographic software.

SECURITY LEVEL

The security level determines the protocols and ciphers that will be supported by the system.

○ Modern	Supports TLS 1.3 only. Provides the highest level of security without providing backward compatibility for older clients.
● Secure	Supports only secure protocols (TLS 1.2 and higher) and ciphers. Recommended for most systems, provides the best balance of security and compatibility.
○ Legacy	Adds support for older ciphers that are no longer considered secure (TLS 1.2 and higher). Only recommended as a last resort if clients do not support secure ciphers.

ADVANCED

□ Use a different security level for connections to internal systems Internal security level: Modern	You can use a different security level for connections to internal systems such as authentication servers (AD/LDAP), SMTP servers, etc. Use this option if internal systems do not support modern and secure encryption standards. To include TLS 1.0 and 1.1, use Obsolete.

Prefer ciphers that:

● Provide the highest level of security	Prefer 256-bit ciphers
○ Allow the highest level of performance and capacity	Prefer 128-bit ciphers

Client Access

Use these features to control a user’s access to WorkPlace and resources.

Change Timeout Settings

To force users to reauthenticate within a specific length of time, set the **Credential lifetime**. Click **General Settings** in the main AMC navigation menu, and then click **Edit** in the **Appliance options** area. This setting applies to all SSL sessions. To make it also apply to the tunnel client and OnDemand proxy sessions, select **Limit session length to credential lifetime** on the **Network Tunnel Client Settings** page.

Deploy End Point Control Components

Secure Mobile Access’s End Point Control components help protect sensitive data and ensure that your network is not compromised when accessed by PCs in untrusted environments.

Use Chained Authentication

For increased security, you can require Connect Tunnel users and users with Web-based access to use two different authentication methods to log in to a single realm. For example, set up RADIUS or a digital certificate as the first authentication method, and LDAP or Active Directory as the second one. See Configuring Chained Authentication for information on how to do this.

Use Strong Two-Factor Authentication Mechanisms, such as TOTP

Two-factor authentication uses two independent means—which are usually something the user has and something the user knows—to establish a user's identity and privileges. For example, you can authenticate users by requiring a TOTP token-code (something the user has) and a password or PIN (something the user knows). See Using Time-Based One-Time Passwords.

Configuring the SAML Identity Provider Service

SMA can be configured as a SAML Identity Provider Service (IdP) to control access and manage single-sign to cloud-based applications.

Prerequisites

SAML is a time-sensitive protocol that requires that your appliance clock to be accurate to function properly. You can help ensure this by enabling an NTP service to keep the network clock on your appliance synchronized.

To enable an NTP service for your appliance:

1. Navigate to **System Configuration > Services**.
2. In the **Network Services** section, under **NTP**, click **Configure**.
3. Click **Enable NTP**.
4. In the **Primary server** field, enter the URL or IP address of NTP server you with which you want to synchronize your appliance.
5. Optionally, in the **Backup server #1** and **Backup server #2** fields enter an URL or IP address of alternate NTP servers. These servers will be used to synchronize your appliance if the primary server is not available.
6. Click **Save**.

Enabling the SAML Identity Provider Service

To enable the SAML Identity Provider Service:

1. Navigate to **System Configuration > Services**.
2. In the **Access Services** section, under **SAML Identity Provider**, click **Configure**.
3. Select **Enable SAML 2.0 Identity Provider service**.
4. In the **Entity ID** field, provide the ID of the Identity Provider (IdP). (In general, the ID will be in an URL format, such as `https://idp.company.com/idp`.)
5. In the **Endpoint FQDN** field, select a Workplace site on which service providers (SAML applications) should send SAML requests to the IdP.

   ⓘ **NOTE:** You can use an existing Workplace site or create a new dedicated Workplace site to use as a dedicated IdP site.
6. In the **Signing certificate** field, the certificate used to signed IdP messages is selected automatically.
7. Click **Save**.
8. You can export SAML metadata of this identity provider by clicking **Export**.

   This metadata contains the endpoints and signing certificate of SMA IdP. It can be imported to your SAML applications to configure their IdP endpoints and certificates.

Configuring the SAML Application

To configure your external web applications:

- The endpoint receiving the SAML login request from the SAML Applications is `https://idp.company.com/samlserver/sso/spinit` (where *`idp.company.com`* is your URL).
- Click **Download** on the **SAML IdP Settings** page to download the certificate used by SMA to sign SAML assertions.

Or, if your SAML application supports it, you can import the IdP metadata by importing the file you exported after configuring your SAML IdP settings. For information on how to do this, refer to Enabling the SAML Identity Provider Service.

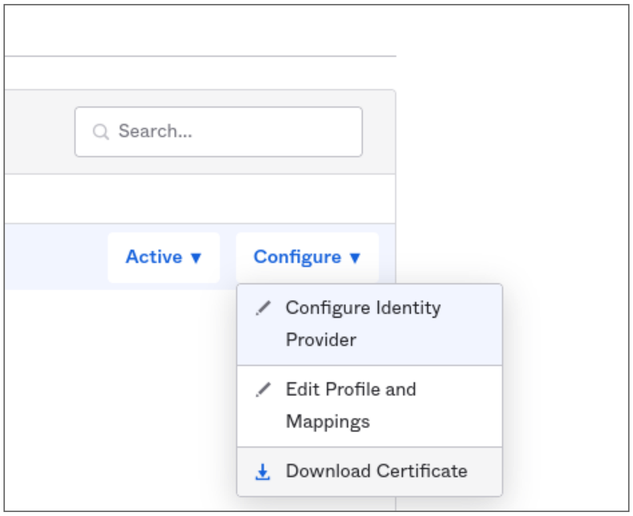
Downloading certificate from service provider

To download metadata xml file from OKTA service provider:

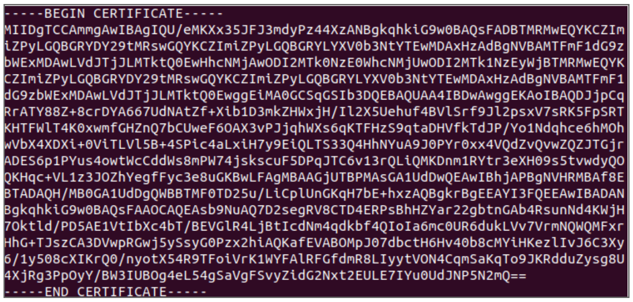
1. Login to OKTA Admin Account.
2. Navigate to **Security** > **Identity Providers** > **Add Identity Provider** > **SAML 2.0**.
3. Configure SAML Identity provider and click **Finish**.

4. Click **Configure**.

5. Click **Download Certificate**.



6. Open the certificate and copy the content of the certificate.



```
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIQU/eMKXx35JFJ3mdyPz44XzANBgkqhkiG9w0BAQsFADBTMRMwEQYKCZIm
iZPyLGQBGRYDY29tMRswGQYKCZImiZPyLGQBGRYLYXV0b3NtYTEwMDAxHzAdBgNVBAMTFmF1dG9z
bWExMDAwLVdJTjJLMTktQ0EwHhcNMjAwODI2MTk0NzE0WhcNMjUwODI2MTk1NzEyWjBTMRMwEQYK
CZImiZPyLGQBGRYDY29tMRswGQYKCZImiZPyLGQBGRYLYXV0b3NtYTEwMDAxHzAdBgNVBAMTFmF1
dG9zbWExMDAwLVdJTjJLMTktQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJjpCq
RrATY88Z+8crDYA667UdNAtZf+Xib1D3mkZHWxjH/Il2X5Uehuf4BVlSrf9Jl2psxV7sRK5FpSRT
KHTFWlT4K0xwmfGHZnQ7bCUweF6OAX3vPJjqhWXs6qKTFHzS9qtaDHVfkTdJP/Yo1Ndqhce6hMOh
wVbX4XDXi+0ViTLVl5B+4SPic4aLxiH7y9EiQLTS33Q4HhNYuA9J0PYr0xx4VQdZvQvwZQZJTGjr
ADES6p1PYus4owtWcCddWs8mPW74jskscuF5DPqJTC6v13rQLiQMKDnm1RYtr3eXH09s5tvwdyQO
QKHqc+VL1z3JOZhYegfFyc3e8uGKBwLFAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBTMF0TD25u/LiCplUnGKqH7bE+hxzAQBgkrBgEEAYI3FQEEAwIBADAN
BgkqhkiG9w0BAQsFAAOCAQEAsb9NuAQ7D2segRV8CTD4ERPsBhHZYar22gbtnGAb4RsunNd4KWjH
7Oktld/PD5AE1VtIbXc4bT/BEVGlR4LjBtIcdNm4qdkbf4QIoIa6mc0UR6dukLVv7VrmNQWQMFxr
HhG+TJszCA3DVwpRGwj5ySsyG0Pzx2hiAQKafEVABOMpJ07dbctH6Hv40b8cMYiHKezlIvJ6C3Xy
6/1y5O8cXIKrQ0/nyotX54R9TFoiVrK1WYFAlRFGfdmR8LIyytVON4CqmSaKqTo9JKRdduZysg8U
4XjRg3PpOyY/BW3IUBOg4eL54gSaVgFSvyZidG2Nxt2EULE7IYu0UdJNP5N2mQ==
-----END CERTIFICATE-----
```

7. Close the certificate.

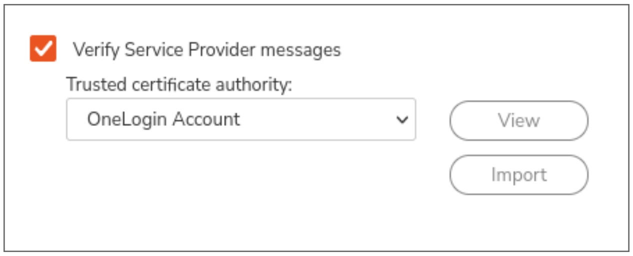
Adding SAML Applications as SAML Resources

Each web application that trusts SMA SAML IdP should be added to SMA as an SAML service provider resource.

To adding an SAML application as an SAML resource:

1. Navigate to **Security Administration > Resources**.
2. On the **Resources** tab, click the **+** (New) icon.
3. Select **SAML service provider** from the dropdown list.
4. In the **Name** field, enter a friendly name for the name of the SAML service provider.
5. In the **Description** field, enter a useful description for the name of the SAML service provider.

6. In the **Entity ID** field, provide the ID of the Identity Provider (IdP). (In general, the ID will be in an URL format, such as https://idp.company.com/idp.)
7. In the **Assertion Consumer Service (ACS) URL** field, enter Assertion Consumer service URL for this SAML application.
8. Select **Create shortcut on WorkPlace** to create a shortcut in WorkPlace to this resource and assign it to a resource group.
9. Click **Advanced** to display the advanced settings.
10. From the **Name ID format** dropdown list, select the appropriate Name ID format for the SAML application.
11. In the **Name ID value** field, compose the Name ID required by the SAML application. You can change or add predefined values by clicking **{variable}**.
12. If the SAML application signs the SAML requests:

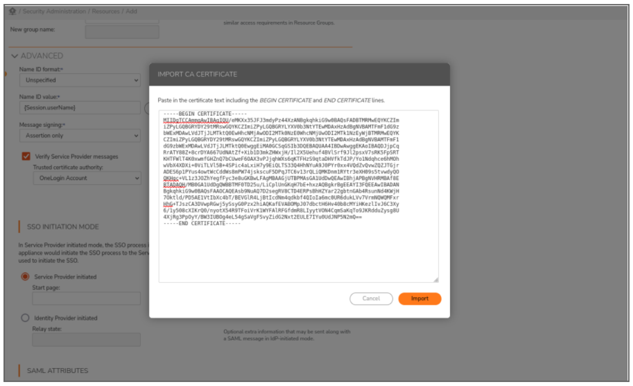


☑ Verify Service Provider messages

Trusted certificate authority: OneLogin Account

   a. Select the **Verify Service Provider messages** checkbox.
   b. In the **Verify Service Provider messages** section do the following:
      1. Click **Import**.

         The **Import Certificate** page is displayed.
      2. Paste the copied certificate and click **Import**.



New group name:

similar access requirements in Resource Groups.

Name ID format:* Unspecified

Name ID value:* {Session.userName}

Message signing:* Assertion only

☑ Verify Service Provider messages

Trusted certificate authority: OneLogin Account

In Service Provider initiated mode, the SSO process i
appliance would initiate the SSO process to the Serv
used to initiate the SSO.

● Service Provider initiated

Start page:

○ Identity Provider initiated

Relay state:

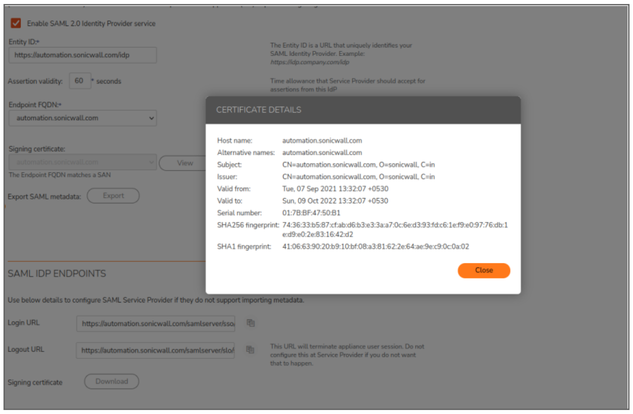
Optional extra information that may be sent along with a SAML message in IdP-initiated mode.

Paste in the certificate text including the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines.

```
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIQU/eMKXx35JFJ3mdyPz44XzANBgkqhkiG9w0BAQsFADBTMRMwEQYKCZIm
iZPyLGQBGRYDY29tMRswGQYKCZImiZPyLGQBGRYLYXV0b3NtYTEwMDAxHzAdBgNVBAMTFmF1dG9z
bWExMDAwLVdJTjJLMTktQ0EwHhcNMjAwODI2MTk0NzE0WhcNMjUwODI2MTk1NzEyWjBTMRMwEQYK
CZImiZPyLGQBGRYDY29tMRswGQYKCZImiZPyLGQBGRYLYXV0b3NtYTEwMDAxHzAdBgNVBAMTFmF1
dG9zbWExMDAwLVdJTjJLMTktQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJjpCq
RrATY88Z+8crDYA667UdNAtZf+Xib1D3mkZHWxjH/Il2X5Uehuf4BVlSrf9Jl2psxV7sRK5FpSRT
KHTFWlT4K0xwmfGHZnQ7bCUweF60AX3vPJjqhWXs6qKTFHzS9qtaDHVfkTdJP/Yo1Ndqhce6hMOh
wVbX4XDXi+0ViTLVl5B+4SPic4aLxiH7y9EiQLTS33Q4HhNYuA9J0PYr0xx4VQdZvQvwZQZJTGjr
ADES6p1PYus4owtWcCddWs8mPW74jskscuF5DPqJTC6v13rQLiQMKDnm1RYtr3eXH09s5tvwdyQ0
QKHgc+VL1z3J0ZhYegfFyc3e8uGKBwLFAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBTMF0TD25u/LiCplUnGKqH7bE+hxzAQBgkrBgEEAYI3FQEEAwIBADAN
BgkqhkiG9w0BAQsFAAOCAQEAsb9NuAQ7D2segRV8CTD4ERPsBhHZYar22gbtnGAb4RsunNd4KWjH
70ktld/PD5AE1VtIbXc4bT/BEVGlR4LjBtIcdNm4qdkbf4QIoIa6mc0UR6dukLVv7VrmNQWQMFxr
HhG+TJszCA3DVwpRGwj5ySsyG0Pzx2hiAQKafEVABOMpJ07dbctH6Hv40b8cMYiHKezlIvJ6C3Xy
6/1y508cXIKrQ0/nyotX54R9TFoiVrK1WYFAlRFGfdmR8LIyytVON4CqmSaKqTo9JKRdduZysg8U
4XjRg3PpOyY/BW3IUBOg4eL54g5aVgF5vyZidG2Nxt2EULE7IYu0UdJNP5N2mQ==
-----END CERTIFICATE-----
```

      3. Click **View**.

The certificate details is displayed.



☑ Enable SAML 2.0 Identity Provider service

Entity ID:* https://automation.sonicwall.com/idp

The Entity ID is a URL that uniquely identifies your SAML Identity Provider. Example: *https://idp.company.com/idp*

Assertion validity: 60 * seconds

Time allowance that Service Provider should accept for assertions from this IdP

Endpoint FQDN:* automation.sonicwall.com

Signing certificate: automation.sonicwall.com

The Endpoint FQDN matches a SAN

Export SAML metadata:

CERTIFICATE DETAILS

Host name: automation.sonicwall.com
Alternative names: automation.sonicwall.com
Subject: CN=automation.sonicwall.com, O=sonicwall, C=in
Issuer: CN=automation.sonicwall.com, O=sonicwall, C=in
Valid from: Tue, 07 Sep 2021 13:32:07 +0530
Valid to: Sun, 09 Oct 2022 13:32:07 +0530
Serial number: 01:7B:BF:47:50:B1
SHA256 fingerprint: 74:36:33:b5:87:cf:ab:d6:b3:e3:3a:a7:0c:6e:d3:93:fd:c6:1e:f9:e0:97:76:db:1e:d9:e0:2e:83:16:42:d2
SHA1 fingerprint: 41:06:63:90:20:b9:10:bf:08:a3:81:62:2e:64:ae:9e:c9:0c:0a:02

SAML IDP ENDPOINTS

Use below details to configure SAML Service Provider if they do not support importing metadata.

Login URL: https://automation.sonicwall.com/samlserver/sso/

Logout URL: https://automation.sonicwall.com/samlserver/slo/

This URL will terminate appliance user session. Do not configure this at Service Provider if you do not want that to happen.

Signing certificate

c. From the **Trusted certificate authority** list, select the certificate to be used to verify the SAML application messages.

   ⓘ **NOTE:** The certificate you want to use must already be imported. For information on importing certificates, refer to Importing CA Certificates.

13. The SMA SAML IdP supports both service provider-initiated and IdP-initiated login (SSO).

   - If the SAML application supports only IdP-initiated SSO:

     1. In the **SSO Initiation Mode** section, select **Identity Provider initiated**. Choosing this option will place a shortcut on the WorkPlace home page users can click in order to log in to the application.

     2. Optionally, You can optionally provide a "Relay state" value if this application needs one.

   - If this application supports service provider-initiated login, you can also optionally provide a start page for the SAML application that will be shown on Workplace home page if you selected **Create shortcut on WorkPlace**.

14. If the SAML application needs extra attributes in addition to the ones already specified in the fields previously completed, you can define them in the **SAML Attributes** section:

   a. Click the **+** (New) icon to enter attribute names and values. You can use **{variable}** to include any of the session variables.

   b. To send an AD attribute, you need to define it first by creating a resource variable. (Refer to Using Variables in Resource and WorkPlace Shortcut Definitions for information on creating resource variables.) You can also perform post-processing on this value before sending to the SAML application, such as searching for and replacing a string in a value. You can then select this variable as a value in the **SAML Attributes** section.

   If you add multiple values with same attribute Name, they will be sent to the SAML application as a multi-valued attribute.

15. Click **Save**.

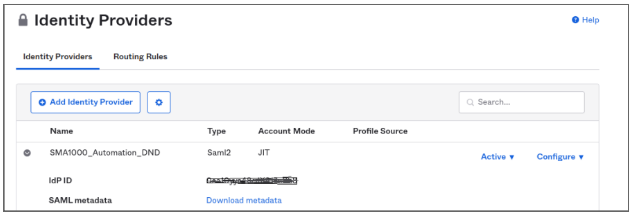
Now you can add this SAML service provider to a resource group like any other internal resources and create access rules to manage it. When users log into WorkPlace, they should see a shortcut to the SAML application, when they have access to SAML resources.

When user reaches SMA for authentication, SMA will evaluate the access rules before sending a SAML Assertion to the application. When allowed, they should be able to successfully log in to SAML applications. Otherwise, they will be denied access and a warning will be displayed.

Downloading metadata from SAML service provider

An example to download metadata xml file from OKTA is as follows:

1. Login to OKTA Admin Account.
2. Navigate to **Security** > **Identity Providers** > **Add Identity Provider** > **SAML 2.0**.
3. Configure SAML Identity provider and click **Finish.**
4. In **Identity Provider** page, click **Add Identity Provider**.
5. Click **Download metadata**.



Name	Type	Account Mode	Profile Source
SMA1000_Automation_DND	Saml2	JIT	

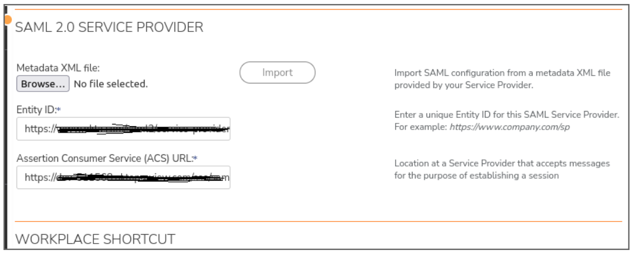
IdP ID [redacted]

SAML metadata Download metadata

Importing metadata in AMC

1. Navigate to **Security Administration** > **Resources**.
2. On the **Resources** tab, click the + (New) icon.
3. Select **SAML service provider** from the dropdown list.
4. In the **Name** field, enter a friendly name for the name of the SAML service provider.
5. In the **Description** field, enter a useful description for the name of the SAML service provider.
6. Click **Browse** and select the metadata xml file to upload.
7. Click **Import**.

   The certificate is imported and the **Entity ID** and **Assertion Consumer Service (ACS) URL** are auto-populated with the URLs.



SAML 2.0 SERVICE PROVIDER

Metadata XML file: Browse... No file selected.

Import

Import SAML configuration from a metadata XML file provided by your Service Provider.

Entity ID:* https://[redacted]

Enter a unique Entity ID for this SAML Service Provider. For example: *https://www.company.com/sp*

Assertion Consumer Service (ACS) URL:* https://[redacted]

Location at a Service Provider that accepts messages for the purpose of establishing a session

WORKPLACE SHORTCUT

8. Click **Save** and apply changes.

Configuring External SAML Identity Providers

This appendix describes how to configure Security Assertion Markup Language (SAML) Identity Providers on an SMA Authentication Server.

ⓘ **NOTE:** The Identity Provider User Interface (UI) pages are subject to change without notice, and may be different than the UI pages used as examples in this document.

Some of configuration procedures in this document require that you download and install a security certificate from the internet before you can complete the procedure. The correct certificate must be available for selection from the **Trust the following certificate** drop-down menu on the **Configure Authentication Server** of the **System Configuration > Authentication Servers** page on the SMA appliance.

The Downloading a Certificate procedure must be done before you can complete the configuration procedures in this document. Which certificate you need is given in the configuration procedure for the specific Identity Provider (IdP). See Configuring SAML Authentication Servers.

Topics:

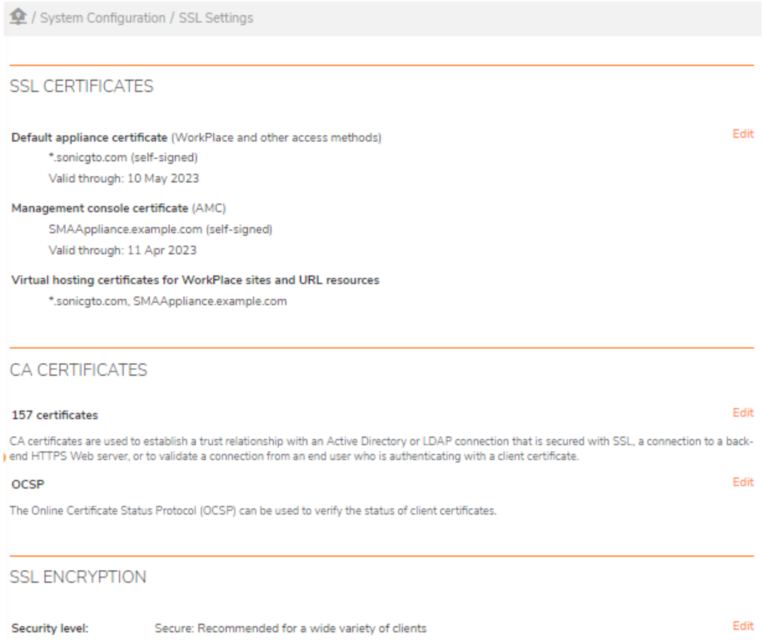
- Downloading a Certificate
- Configuring SAML Authentication Servers

Downloading a Certificate

This procedure must be done before you can select a certificate from the **Trust the following certificate** drop-down menu in the configuration procedures.

To download and install a certificate:

1. Download the certificate you want from the **Configure Single Sign-on at <*APP_NAME*>** page that appears during the application registration.
2. In the AMC, navigate to **System Configuration > SSL Settings**.



SSL CERTIFICATES

Default appliance certificate (WorkPlace and other access methods)
*.sonicgto.com (self-signed)
Valid through: 10 May 2023

Edit

Management console certificate (AMC)
SMAAppliance.example.com (self-signed)
Valid through: 11 Apr 2023

Virtual hosting certificates for WorkPlace sites and URL resources
*.sonicgto.com, SMAAppliance.example.com

CA CERTIFICATES

157 certificates

Edit

CA certificates are used to establish a trust relationship with an Active Directory or LDAP connection that is secured with SSL, a connection to a back-end HTTPS Web server, or to validate a connection from an end user who is authenticating with a client certificate.

OCSP

Edit

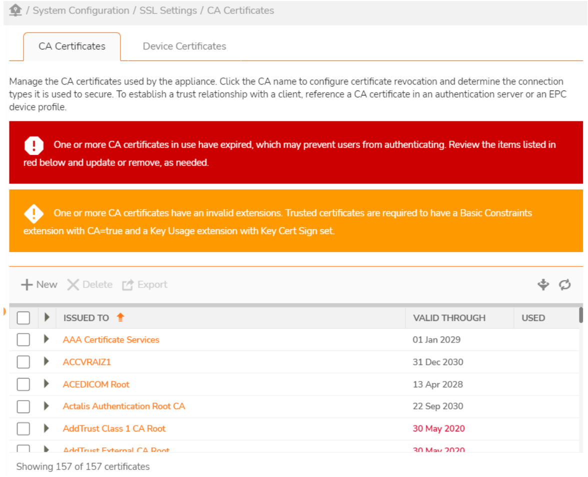
The Online Certificate Status Protocol (OCSP) can be used to verify the status of client certificates.

SSL ENCRYPTION

Security level: Secure: Recommended for a wide variety of clients

Edit

3. In the **CA Certificates** section, click **Edit** for **<*number*> certificates**. The **CA Certificates** page displays.



Manage the CA certificates used by the appliance. Click the CA name to configure certificate revocation and determine the connection types it is used to secure. To establish a trust relationship with a client, reference a CA certificate in an authentication server or an EPC device profile.

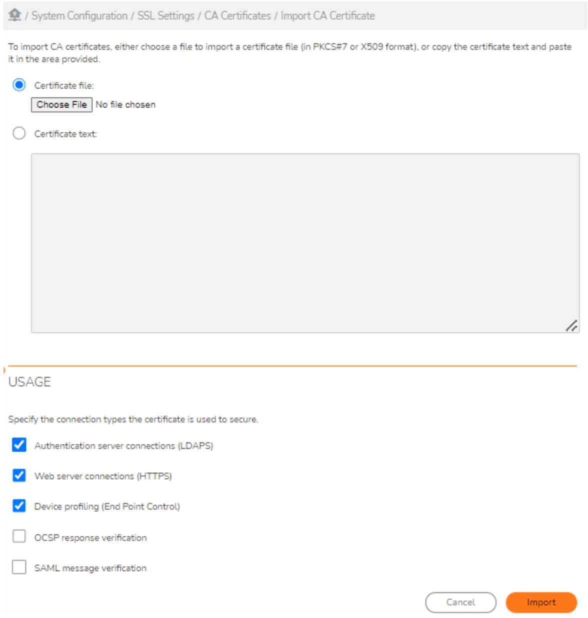
One or more CA certificates in use have expired, which may prevent users from authenticating. Review the items listed in red below and update or remove, as needed.

One or more CA certificates have an invalid extensions. Trusted certificates are required to have a Basic Constraints extension with CA=true and a Key Usage extension with Key Cert Sign set.

□		ISSUED TO	VALID THROUGH	USED
□	▸	AAA Certificate Services	01 Jan 2029	
□	▸	ACCVRAIZ1	31 Dec 2030	
□	▸	ACEDICOM Root	13 Apr 2028	
□	▸	Actalis Authentication Root CA	22 Sep 2030	
□	▸	AddTrust Class 1 CA Root	30 May 2020	
□	▸	AddTrust External CA Root	30 May 2020	

Showing 157 of 157 certificates

4. Click the **+** (New) icon. The **Import CA Certificate** page displays.



/ System Configuration / SSL Settings / CA Certificates / Import CA Certificate

To import CA certificates, either choose a file to import a certificate file (in PKCS#7 or X509 format), or copy the certificate text and paste it in the area provided.

● Certificate file:

No file chosen

○ Certificate text:

USAGE

Specify the connection types the certificate is used to secure.

☑ Authentication server connections (LDAPS)

☑ Web server connections (HTTPS)

☑ Device profiling (End Point Control)

□ OCSP response verification

□ SAML message verification

5. Select one of the following options:

   a. **Certificate file** and browse to select the certificate you want.

   b. **Certificate text** and enter the certificate text that you want.

6. Click **Import**.

   The certificate should now appear in the **Trust the following certificate** drop-down menu.

Configuring SAML Authentication Servers

This section describes how to configure the various SAML Authentication Servers (IDP).

Some of these configuration procedures require that you already have certain certificates downloaded and installed on your SMA appliance, so that they are available from the **Trust the following certificate** drop-down menu. See Downloading a Certificate for details on how to do this.

Topics:

- Azure Active Directory
- Integrating SMA with Duo SSO Server using SAML
- Integrating with Duo Access Gateway Serverusing SAML
- One Identity Cloud Access Manager
- OneLogin
- Ping Identity PingOne
- Salesforce

Azure Active Directory

This section describes how to configure the Azure Active Directory (AD) as an SMA Authentication Server.

Topics:

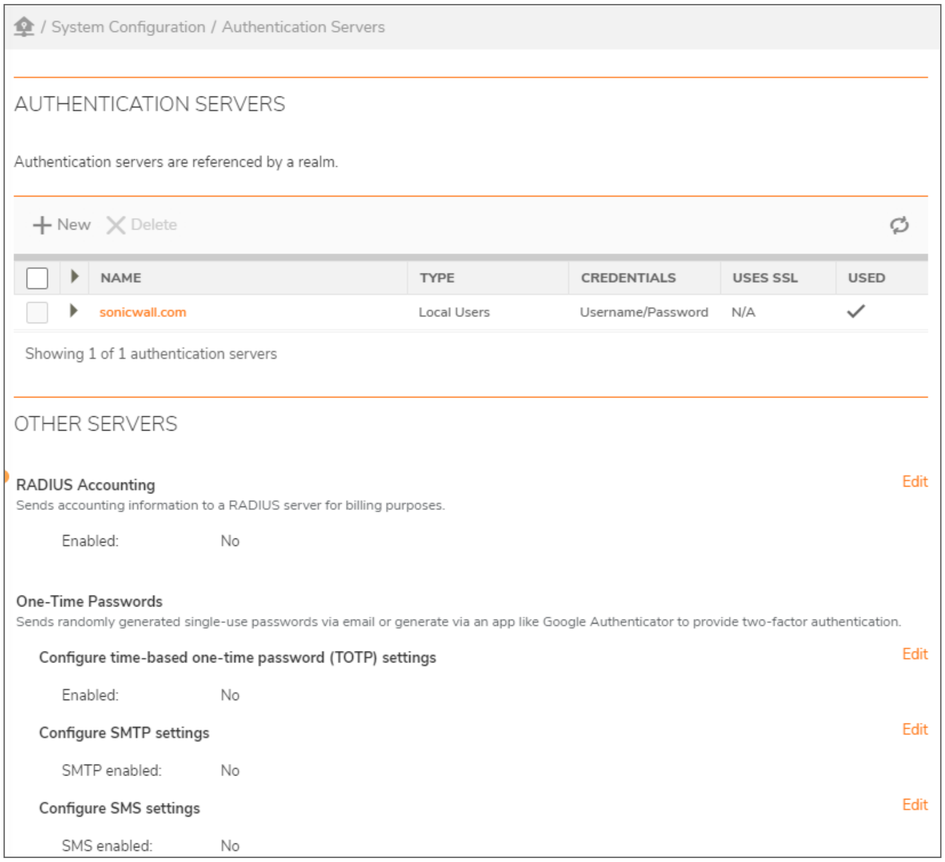
- Configuring Azure Active Directory as an SMA Authentication Server
- Adding the SMA Application to Azure Active Directory
- Configuring Azure Active Directory as an SAML Identity provider
- Assigning Users and Groups to the SMA Application
- Sending User Groups to SMA

Configuring Azure Active Directory as an SMA Authentication Server

Using this procedure you can create and configure an Authentication server on an SMA appliance and configure Azure AD as an SAML Identity provider.

To configure Azure AD as an SMA Authentication Server, do the following:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

□		NAME	TYPE	CREDENTIALS	USES SSL	USED
□	▸	sonicwall.com	Local Users	Username/Password	N/A	✓

Showing 1 of 1 authentication servers

OTHER SERVERS

RADIUS Accounting
Sends accounting information to a RADIUS server for billing purposes.

Enabled: No

One-Time Passwords
Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings

Enabled: No

Configure SMTP settings

SMTP enabled: No

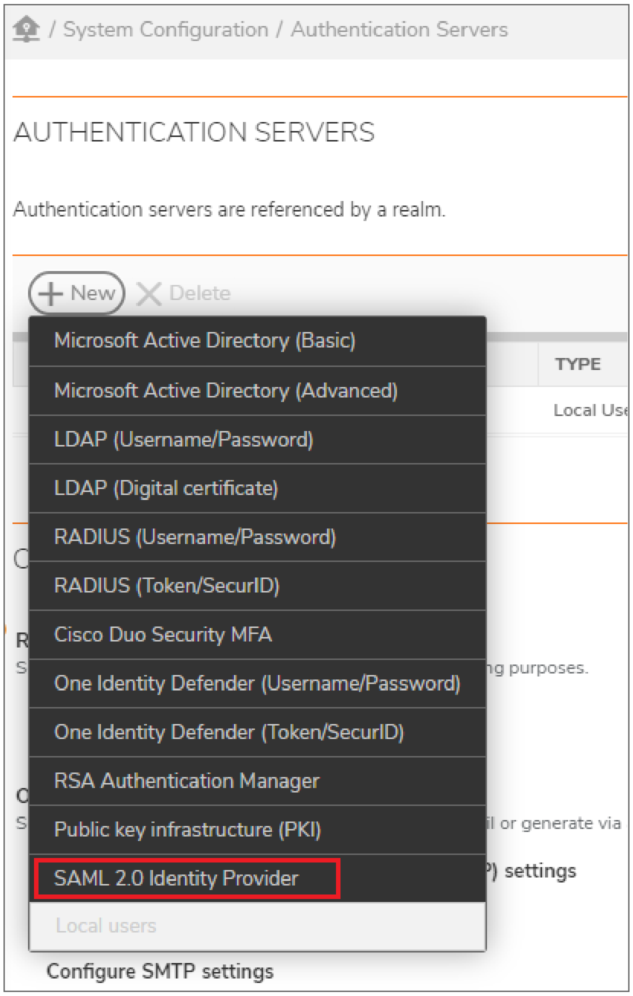
Configure SMS settings

SMS enabled: No

2. Under **Authentication servers**, click **New**.

   The **Add Authentication Server** page displays.

3. Select **SAML 2.0 Identity Provider**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
TYPE
Local Use
ng purposes.
il or generate via
) settings
Configure SMTP settings

4. In the **Name** field, type a friendly name. For example, **Azure**.
5. In the **Appliance ID** option provide an appliance URL. For example, `https://workplace.company.com/`. (This can be of any value, but an URL is recommended).
6. For **Endpoint FQDN** option, select a **workplace.company.com** from drop-down menu.

   The value for **Assertion Consumer Service (ACS) URL** is formed automatically based on **Endpoint FQDN** value.
7. Click **Export** to download the appliance configuration as a SAML metadata file.

   The .xml file is downloaded.
8. While you have the SMA application tab active, open a new window in the browser to configure Azure AD in Azure portal.
9. To add the SMA application to the Azure AD service, go to Adding the SMA Application to Azure Active Directory.

Adding the SMA Application to Azure Active Directory

After you configure Azure Active Directory (AD) as an SMA Authentication Server, you need to add the SMA application to the Azure AD service.

To add the SMA application to the Azure AD service, do the following:

1. Login to Azure Portal.
2. Select **Azure Active Directory > Enterprise applications**.
3. Click **New application**> **Create your own application**.
4. Enter the name of the application, for example, `SMA1000 VPN (239)`, and select **Non-gallery application** option.
5. Click **Create**.
6. In the **Manage** > **Self-Service**, click **Set up single sign on** > **SAML**.
7. Click **upload metadata file** and browse to upload the .xml file downloaded in Configuring Azure Active Directory as an SMA Authentication Server.
8. Click **Add**to upload the xml file.
9. Review the **Identifier (Entity ID)** and **Reply URL**.
10. Click **Save**.
11. If needed, under **Attributes and Claims**, edit the required attributes.
12. Under **SAMLCertificates**, download the Federation Metadata XML.

    The .xml file is downloaded.

    > **NOTE:** For the most current information for configuring Azure, refer to https://learn.microsoft.com/en-in/azure/active-directory/manage-apps/view-applications-portal.

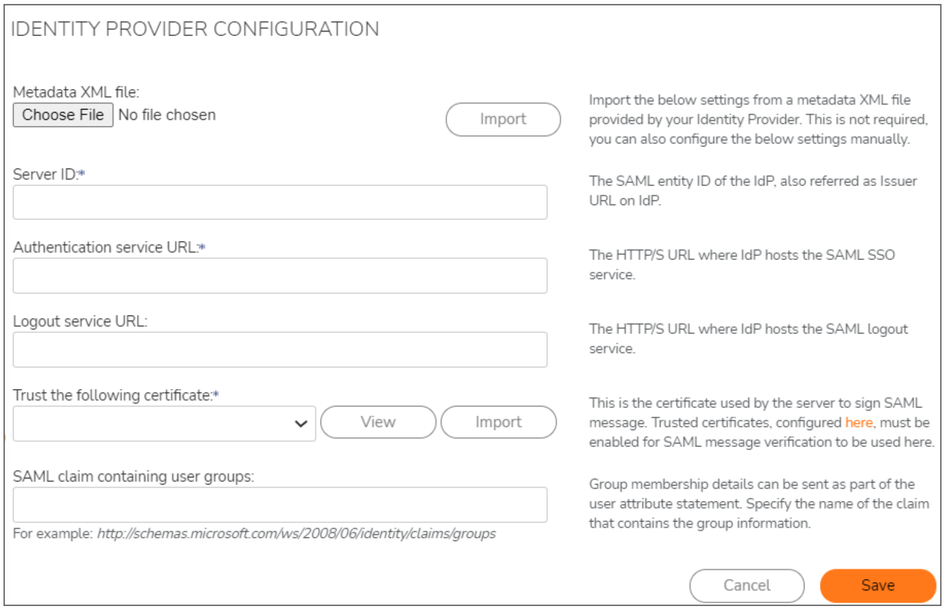
13. Go to the SMA application window to configure the SAML Authentication server. See Configuring Azure Active Directory as an SAML Identity provider.

Configuring Azure Active Directory as an SAML Identity provider

In this procedure, you will configure Azure AD as an SAML Identity provider, and create and configure an Authentication server on an SMA appliance.

To configure Azure AD as an SAML Identity provider, do the following:

1. Under **Identity Provider Configuration**, click **Choose File** and select the downloaded metadata.xml in



IDENTITY PROVIDER CONFIGURATION

Metadata XML file: No file chosen

Import the below settings from a metadata XML file provided by your Identity Provider. This is not required, you can also configure the below settings manually.

Server ID:*

The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:*

The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL:

The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:*

This is the certificate used by the server to sign SAML message. Trusted certificates, configured here, must be enabled for SAML message verification to be used here.

SAML claim containing user groups:

For example: *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*

Group membership details can be sent as part of the user attribute statement. Specify the name of the claim that contains the group information.

2. Click **Import**.

   All the IDP configuration fields are filled with the respective values including IDP certificate.

   Options **Server ID**, **Authentication service URL** and **Trust the following certificate** should be automatically filled based on uploaded file.

   ⓘ **NOTE:** When you are importing the metadata file under authentication server, the CA certificate for SAML verification is enabled by default. In addition, the imported CA certificates under **SSL Settings > CA Certificate** with SAML verification enabled will be displayed.

   ⓘ **NOTE:** The **Logout service URL** field is for logging out IDP and SAML together. However if you can keep this field empty, so that the IDP remains active and only SAML application gets logged out.

3. Click **Save**.

Assigning Users and Groups to the SMA Application

After the SMA application has been configured to use Azure AD as an SAML-based Identity Provider, then it is almost ready to test. As a security control, Azure AD will not issue a token allowing users to sign into the SMA application until they have been granted access using Azure AD, either directly or through a group.

To assign a user or group to the SMA application:

1. In Azure AD, click the **Assign Users** button.
2. Select the user or group you wish to assign, and then select the **Assign** button.

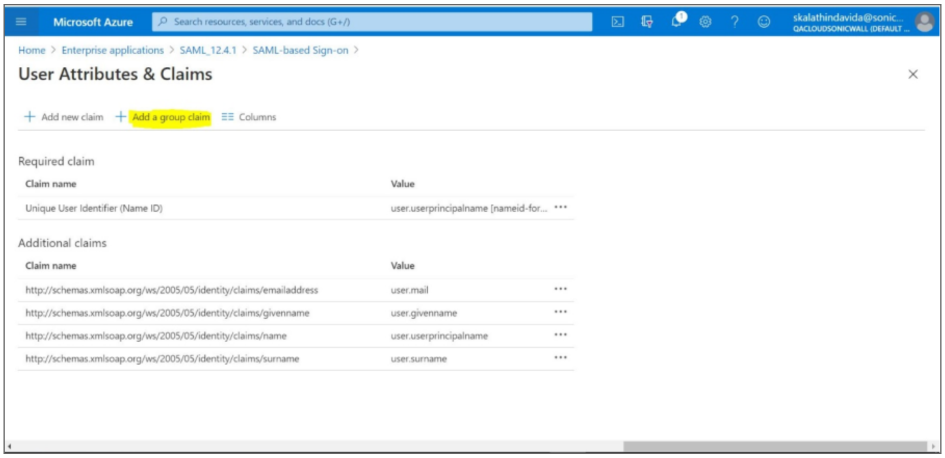
Sending User Groups to SMA

After configuring individual user ID, you can also now send group details to SMA for group level management. You can add a group claim and send the list of groups the user is member of.

To send user groups to SMA, add a group claim.:

1. To add a group claim, navigate to **SAML application > Single sign on > Edit User attribute and Claim > Add a group claim**.

   This evaluates group membership and provides access to resources, which serves IDP to share all the group membership information to SMA in the SAML response.



Microsoft Azure
Search resources, services, and docs (G+/)
skalathindavida@sonic...
QACLOUDSONICWALL (DEFAULT ...

Home > Enterprise applications > SAML_12.4.1 > SAML-based Sign-on >

User Attributes & Claims

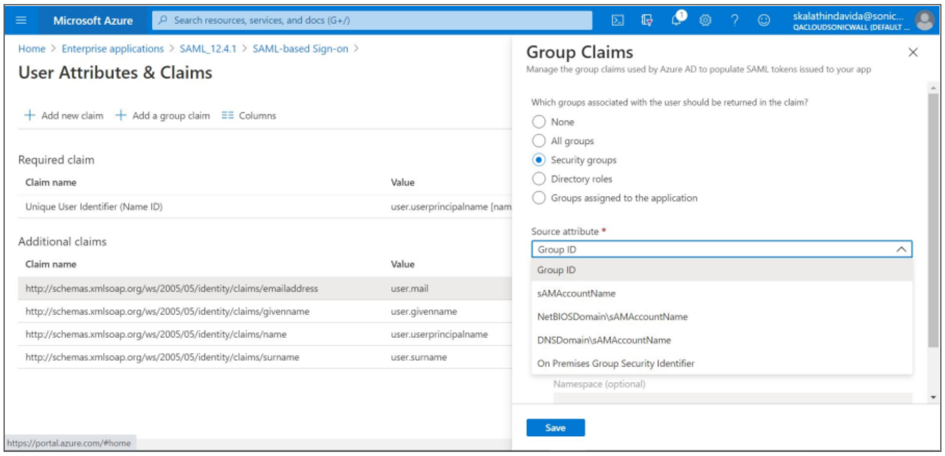
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

2. Select the group (for example, select Security groups) and source attribute (for example, select Group ID) for the group based on your requirements and click **Save**.



Microsoft Azure
Search resources, services, and docs (G+/)
skalathindavida@sonic...
QACLOUDSONICWALL (DEFAULT ...

Home > Enterprise applications > SAML_12.4.1 > SAML-based Sign-on >

User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nam

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
● Security groups
○ Directory roles
○ Groups assigned to the application

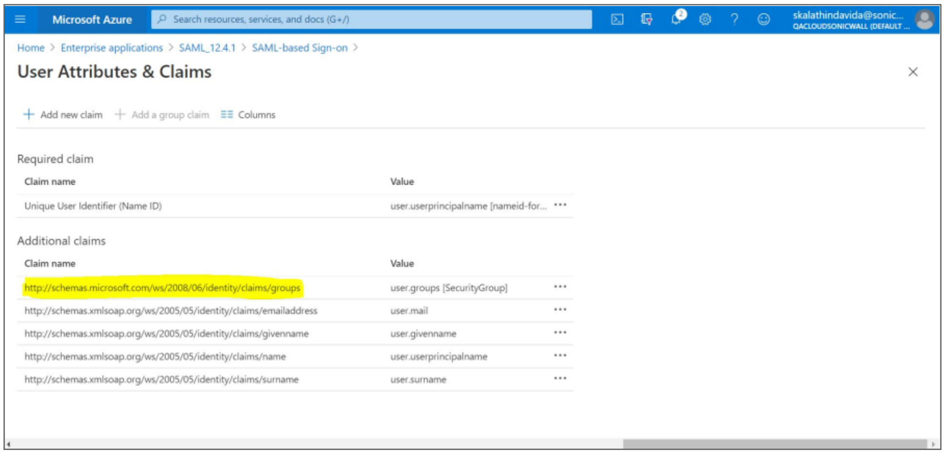
Source attribute *

Group ID

Group ID
sAMAccountName
NetBIOSDomain\sAMAccountName
DNSDomain\sAMAccountName
On Premises Group Security Identifier
Namespace (optional)
Save
https://portal.azure.com/#home

   A group claim name *"http://schemas.microsoft.com/ws/2008/06/identity/claims/groups"* is created.

3. Copy this group claim name and in SMA AMC enter in SAML claim containing user groups field under **Authentication Servers** > **Edit Authentication Server** > **Identity Provide Configuration.** For more information refer to Configuring a SAML 2.0 Identity Provider Authentication Server.



Microsoft Azure
Search resources, services, and docs (G+/)
skalathindavida@sonic...
QACLOUDSONICWALL (DEFAULT ...
Home > Enterprise applications > SAML_12.4.1 > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim
+ Add a group claim
Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [SecurityGroup]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

4. To use the groups under **ACL** or **Community**, you will need to add them under **Security Administration** > **Users & Groups** > **Mapped Accounts**.

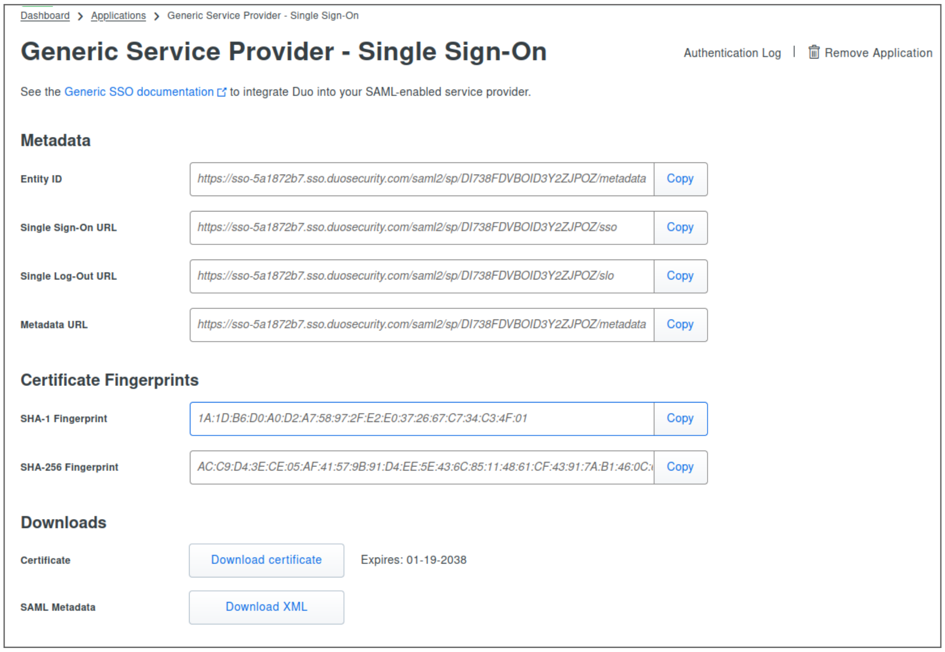
   ⓘ **NOTE:** For Azure you can use group's **Object ID** as Group name in SMA under **Users & Groups**> **Edit Mapped Account**.

To configure the group details in AMC refer to the Adding Users or Groups Manuallysection.

Integrating SMA with Duo SSO Server using SAML

This section explains the procedure to configure Duo SSO Server (cloud) as Authentication server for SMA1000 using SAML Protocol.

1. On Duo admin portal, select **Applications** > **Protect an Application**.
2. On the search filter under **Protect an Application**, search for **Generic Service Provider** and select the application with protection type as **2FA with SSO hosted by Duo (Single Sign-On)**.
3. Under **Downloads**, click the **Download XML** button to download Duo metadata file.



Dashboard > Applications > Generic Service Provider - Single Sign-On

Generic Service Provider - Single Sign-On

Authentication Log | Remove Application

See the Generic SSO documentation to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DI738FDVBOID3Y2ZJPOZ/metadata Copy

Single Sign-On URL https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DI738FDVBOID3Y2ZJPOZ/sso Copy

Single Log-Out URL https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DI738FDVBOID3Y2ZJPOZ/slo Copy

Metadata URL https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DI738FDVBOID3Y2ZJPOZ/metadata Copy

Certificate Fingerprints

SHA-1 Fingerprint 1A:1D:B6:D0:A0:D2:A7:58:97:2F:E2:E0:37:26:67:C7:34:C3:4F:01 Copy

SHA-256 Fingerprint AC:C9:D4:3E:CE:05:AF:41:57:9B:91:D4:EE:5E:43:6C:85:11:48:61:CF:43:91:7A:B1:46:0C: Copy

Downloads

Certificate Download certificate Expires: 01-19-2038

SAML Metadata Download XML

4. On SMA AMC page, create a SAML Authentication server under **Authentication servers** > **New** > **SAML 2.0 Identity Provider** > **Continue**.

   a. In the **Name** field, type a friendly name. For example, **Duo SSO Server**.

   b. In the **Appliance ID** option provide an appliance URL. For example, https://sma.company.com/. (This can be of any value, but an URL is recommended).

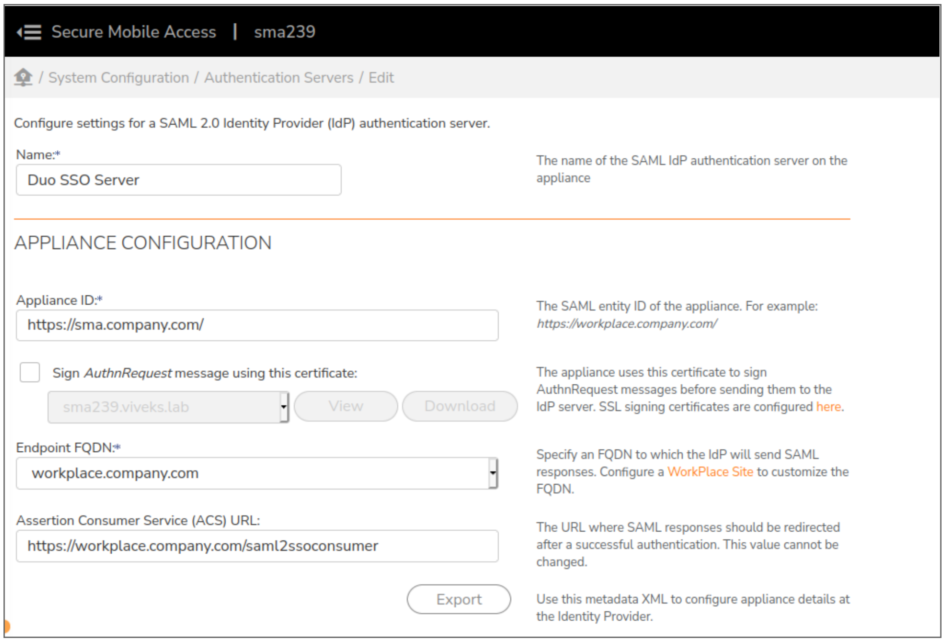
   c. Clear the **Sign AuthnRequest message using this certificate** option.

   d. For **Endpoint FQDN** option, select a **Workplace site FQDN** from drop-down menu.

      This will act as the endpoint for all communications with Duo SSO server. (This is not necessarily be same as Appliance ID value).

      The value for **Assertion Consumer Service (ACS) URL** is formed automatically based on

Endpoint FQDN value.



Secure Mobile Access | sma239

/ System Configuration / Authentication Servers / Edit

Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name:* Duo SSO Server — The name of the SAML IdP authentication server on the appliance

APPLIANCE CONFIGURATION

Appliance ID:* https://sma.company.com/ — The SAML entity ID of the appliance. For example: *https://workplace.company.com/*

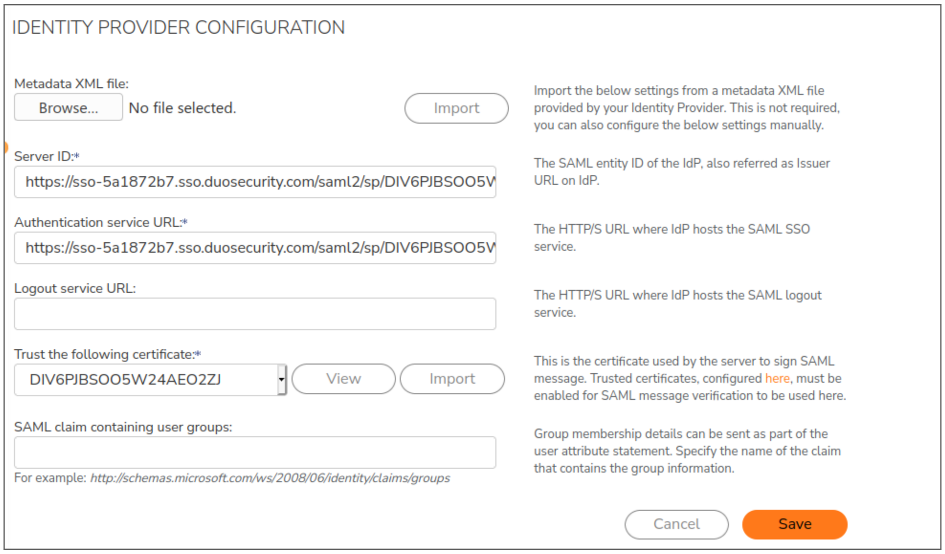
□ Sign *AuthnRequest* message using this certificate: sma239.viveks.lab [View] [Download] — The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN:* workplace.company.com — Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

Assertion Consumer Service (ACS) URL: https://workplace.company.com/saml2ssoconsumer — The URL where SAML responses should be redirected after a successful authentication. This value cannot be changed.

[Export] — Use this metadata XML to configure appliance details at the Identity Provider.

5. Under **Identity Provider Configuration** section, under **Metadata XML file** option, click browse and select the `Duo metadata` file downloaded earlier.
   a. Click **Import** to upload the metadata.
   b. Options **Server ID**, **Authentication service URL** and **Trust the following certificate** should be automatically filled based on uploaded file.
   c. Clear **Logout service URL** textbox if needed.
   d. Click **Save** button and assign this authentication server to any realm.



IDENTITY PROVIDER CONFIGURATION

Metadata XML file: [Browse...] No file selected. [Import] — Import the below settings from a metadata XML file provided by your Identity Provider. This is not required, you can also configure the below settings manually.

Server ID:* https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DIV6PJBSOO5V — The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:* https://sso-5a1872b7.sso.duosecurity.com/saml2/sp/DIV6PJBSOO5V — The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL: — The HTTP/S URL where IdP hosts the SAML logout service.

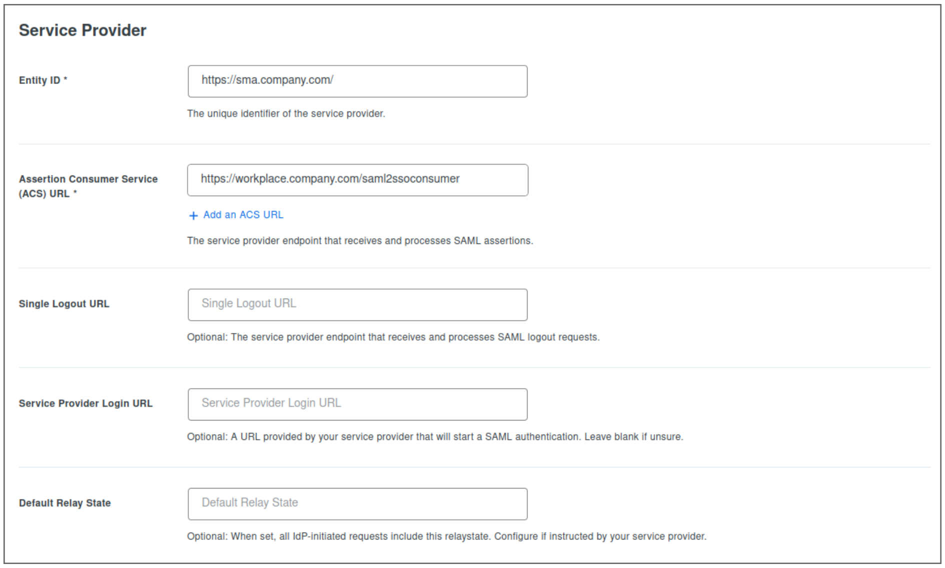
Trust the following certificate:* DIV6PJBSOO5W24AEO2ZJ [View] [Import] — This is the certificate used by the server to sign SAML message. Trusted certificates, configured here, must be enabled for SAML message verification to be used here.

SAML claim containing user groups: — Group membership details can be sent as part of the user attribute statement. Specify the name of the claim that contains the group information.

For example: *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*

[Cancel] [Save]

6. On Duo admin portal, under **Service Provider** section, for **Entity ID** option, use the **Appliance ID** value from SMA configuration. For example *https://sma.company.com/*.
7. For **Assertion Consumer Service (ACS) URL**, use the **Assertion Consumer Service (ACS) URL** value from SMA configuration. Example: *https://workplace.company.com/saml2ssoconsumer*.
8. Leave all the other options at their default values.
9. Under **SAML Response** section, select the **NameID format** as **emailAddress**.



Service Provider

Entity ID * : https://sma.company.com/
The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL * : https://workplace.company.com/saml2ssoconsumer

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL : Single Logout URL
Optional: The service provider endpoint that receives and processes SAML logout requests.

Service Provider Login URL : Service Provider Login URL
Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State : Default Relay State
Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

10. Under **SAML Response** section, select the **NameID format** as **emailAddress**.
11. Select the **NameID attribute** as **Email Address**.
12. Select the **Signature algorithm** as **SHA256**.
13. For **Signing** options, select both **Sign response** and **Sign assertion** checkboxes.
14. Leave other options at their default values.
15. Click **Save Configuration** button to save the configuration.
16. On the same page, under **Policy and Settings** section, change the values as needed.
17. Click **Save**.

Integrating with Duo Access Gateway Serverusing SAML

This section explains the procedure to configure on-premise Duo Access Server (DAG) as Authentication server for SMA1000 using SAML Protocol.

1. To create a SAML Authentication server on SMA AMC portal, go to **Authentication servers** > **New** >**SAML 2.0 Identity Provider** > **Continue**.

a. In the **Name** field, type a friendly name. For example, **Duo Acess Gateway Server**.

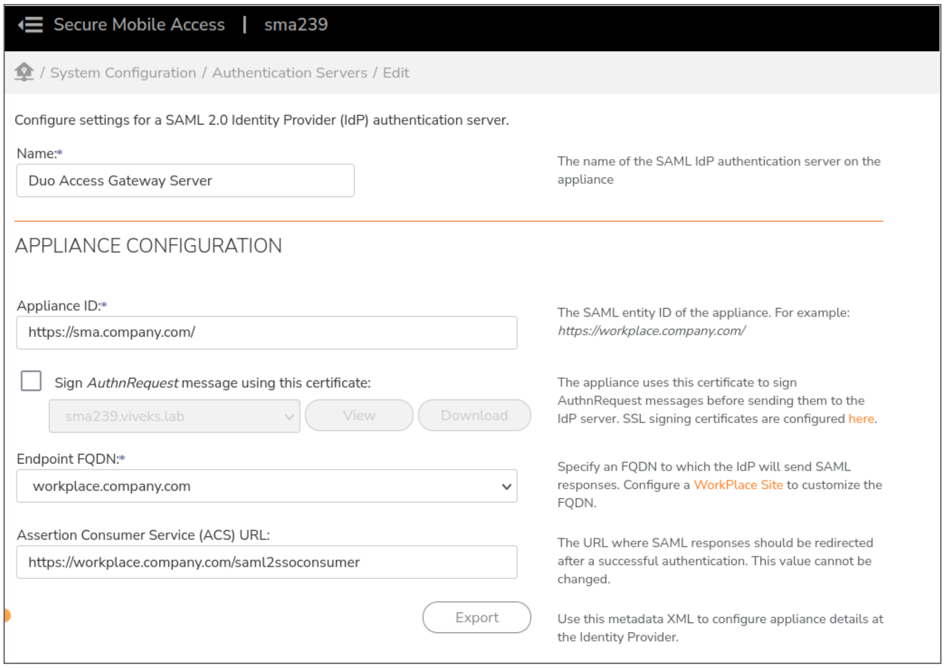
b. In the **Appliance ID** option provide an appliance URL. For example, https://sma.company.com/. (This can be of any value, but an URL is recommended).

c. Clear the **Sign AuthnRequest message using this certificate** option.

d. For **Endpoint FQDN** option, select a **Workplace site FQDN** from drop-down menu.

This will act as the endpoint for all communications with Duo Access Gateway server. (This is not necessarily be same as Appliance ID value)

The value for **Assertion Consumer Service (ACS) URL** is formed automatically based on **Endpoint FQDN** value.


Secure Mobile Access | sma239
/ System Configuration / Authentication Servers / Edit
View
Download
Export

Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name:* Duo Access Gateway Server

The name of the SAML IdP authentication server on the appliance

APPLIANCE CONFIGURATION

Appliance ID:* https://sma.company.com/

The SAML entity ID of the appliance. For example: *https://workplace.company.com/*

□ Sign *AuthnRequest* message using this certificate: sma239.viveks.lab

The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN:* workplace.company.com

Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

Assertion Consumer Service (ACS) URL: https://workplace.company.com/saml2ssoconsumer

The URL where SAML responses should be redirected after a successful authentication. This value cannot be changed.

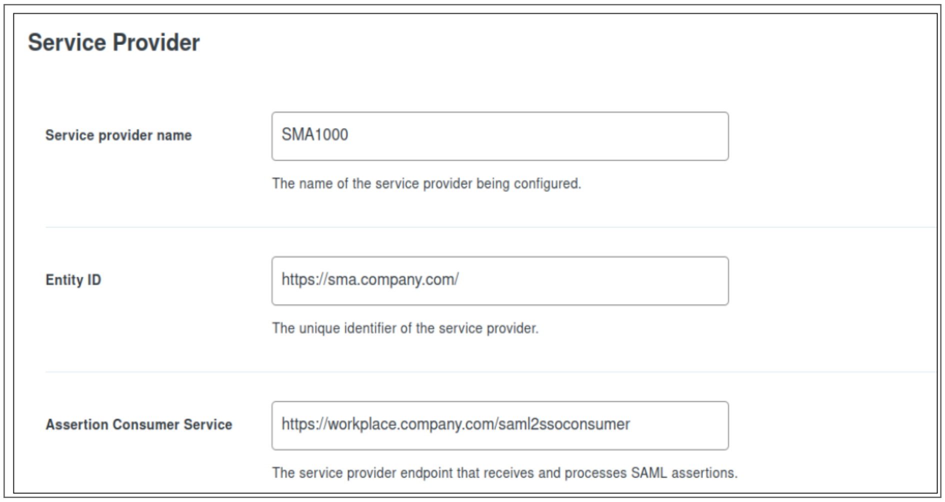
Use this metadata XML to configure appliance details at the Identity Provider.

2. On Duo admin portal, select **Applications** > **Protect an Application**.

a. On the search filter under **Protect an Application**, search for **Generic Service Provider** and select the application with protection type as **2FA with SSO self-hosted (Duo Access Gateway)**.

b. Under **Configure SAML Service Provider** > **Service Provider** section, provide a friendly name.

c. On Duo admin portal, under **Service Provider** section, for **Entity ID** option, use the **Appliance ID** value from SMA configuration. For example *https://sma.company.com/*.



Service Provider

Service provider name: SMA1000
The name of the service provider being configured.

Entity ID: https://sma.company.com/
The unique identifier of the service provider.

Assertion Consumer Service: https://workplace.company.com/saml2ssoconsumer
The service provider endpoint that receives and processes SAML assertions.

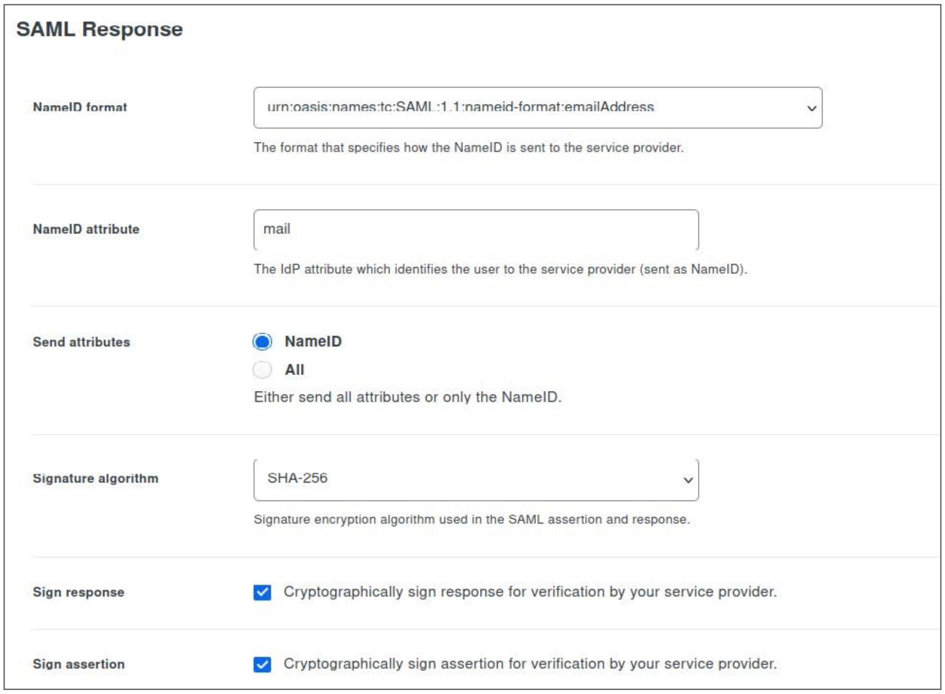
3. For **Assertion Consumer Service (ACS) URL**, use the **Assertion Consumer Service (ACS) URL** value from SMA configuration. Example: *https://workplace.company.com/saml2ssoconsumer*.
4. Leave all the other options at their default values.
5. Under **SAML Response** section, do the following:
   a. Select the **NameID format** as **emailAddress**.
   b. Select the **NameID attribute** as **mail**.

      ⓘ | **NOTE:**

      - **NameID format** and **NameID attribute** values might differ base on authentication source.
      - In case of LDAP authentication source, make sure this **NameID attribute** is actually configured to be retrieved.

   c. Select the **Signature algorithm** as **SHA256**.
   d. For **Signing options**, select both **Sign response** and **Sign assertion** checkboxes.

e. Leave the other options under this section with their default values.



SAML Response

NameID format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

The format that specifies how the NameID is sent to the service provider.

NameID attribute: mail

The IdP attribute which identifies the user to the service provider (sent as NameID).

Send attributes: ● NameID ○ All

Either send all attributes or only the NameID.

Signature algorithm: SHA-256

Signature encryption algorithm used in the SAML assertion and response.

Sign response: ☑ Cryptographically sign response for verification by your service provider.

Sign assertion: ☑ Cryptographically sign assertion for verification by your service provider.

6. Click **Save Configuration**.
7. Go to **Policy** section and change the values as needed and click **Save**.
8. Click **Download your configuration file** link to download the configuration file that will be uploaded to on-premise Duo Access Gateway server
9. On Duo Access Gateway admin console, select **Applications**>**Add Application** > **Choose File** and browse to select the downloaded configuration file.
10. Click **Upload**.
11. In **Metadata** section click **Download XML** metadata link to download Duo SAML metadata file.
12. In AMC, under **Identity Provider Configuration** section, under **Metadata XML file** option, click browse and select the `Duo metadata` file downloaded earlier.
    a. Click **Import** to upload the metadata.
    b. Options **Server ID**, **Authentication service URL** and **Trust the following certificate** should be automatically filled based on uploaded file.
    c. Clear **Logout service URL** textbox if needed.
    d. Click **Save** button and assign this authentication server to any realm.

One Identity Cloud Access Manager

This section describes how to configure One Identity Cloud Access Manager (CAM) 7.0 as an SMA Authentication Server.

Topics:

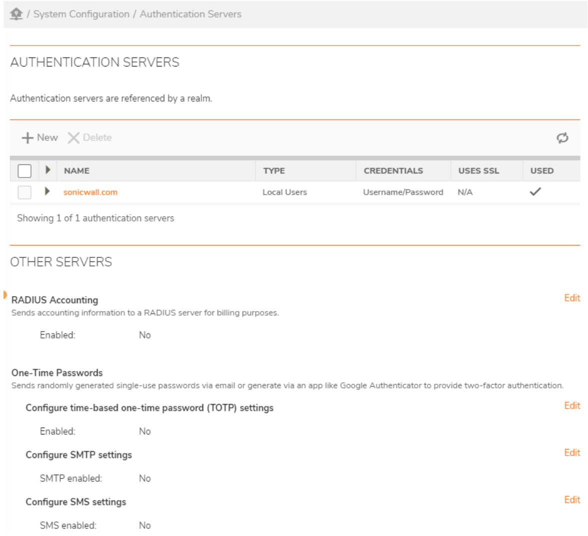
- Configuring One Identity CAM as an SMA Authentication Server
- Adding the SMA Application to One Identity Cloud Access Manager

Configuring One Identity CAM as an SMA Authentication Server

Configuring the One Identity Cloud Access Manager (CAM) as an SMA appliance is done by setting up a One Identity CAM Authentication Server on an SMA appliance.

To configure the One Identity CAM as an SMA Authentication Server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

□	NAME	TYPE	CREDENTIALS	USES SSL	USED
□	sonicwall.com	Local Users	Username/Password	N/A	✓

Showing 1 of 1 authentication servers

OTHER SERVERS

RADIUS Accounting Edit
Sends accounting information to a RADIUS server for billing purposes.

Enabled: No

One-Time Passwords
Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings Edit

Enabled: No

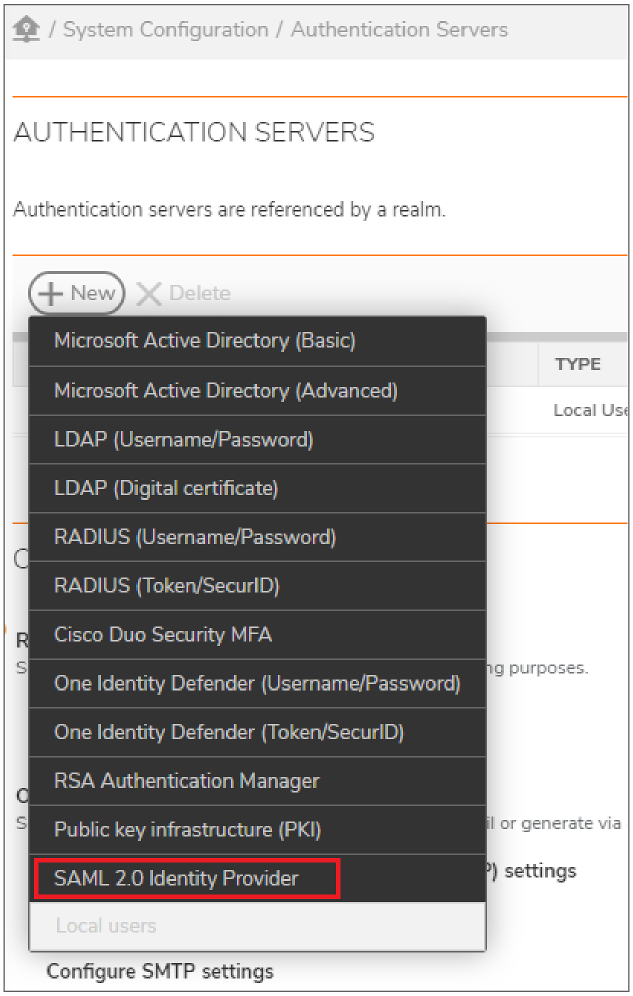
Configure SMTP settings Edit

SMTP enabled: No

Configure SMS settings Edit

SMS enabled: No

2. Under **Authentication servers**, click the **+** (New) icon. The **Add Authentication Server** page displays.



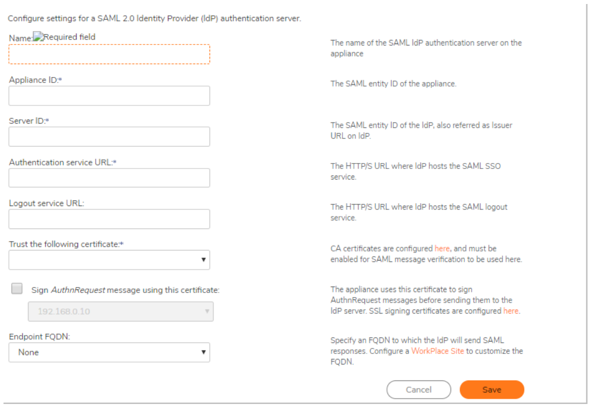
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

+ New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
TYPE
Local Use
ng purposes.
il or generate via
) settings
Configure SMTP settings

3. Select **SAML 2.0 Identity Provider**.
4. Click **Continue....** The **Edit Authentication Server** page displays.



Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name: Required field	The name of the SAML IdP authentication server on the appliance
Appliance ID:*	The SAML entity ID of the appliance.
Server ID:*	The SAML entity ID of the IdP, also referred as Issuer URL on IdP.
Authentication service URL:*	The HTTP/S URL where IdP hosts the SAML SSO service.
Logout service URL:	The HTTP/S URL where IdP hosts the SAML logout service.
Trust the following certificate:*	CA certificates are configured here, and must be enabled for SAML message verification to be used here.
□ Sign *AuthnRequest* message using this certificate: 192.168.0.10	The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.
Endpoint FQDN: None	Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

Some of the values for the fields in the **Configure Authentication Server** page can be obtained from the **Application Created** page of the **One Identity Cloud Access Manager**.

The steps that follow explain how to configure the fields in the **Configure Authentication Server** page.

5. In the **Name** field, enter **CAM**.
6. In the **Appliance ID** field, enter the **Audience/SP Identity** from the **Application Created** page. For example, `https://appliance.company.com`.
7. In the **Server ID** field, enter the **Issuer Entity ID** or **IDP** from the **Application Created** page. For example, `urn:cam.test.com.test.com/CloudAccessManager/RPSTS`.
8. In the **Authentication service URL** field, enter the **IDP Login URL** from the **Application Created** page. For example,

   https://sp16.test.com/CloudAccessManager/RPSTS/Saml2/Default.aspx.
9. In the **Logout service URL** field, enter the **SSO URL**. For example, https://cam.test.com.com/CloudAccessManager/RPSTS/Saml2/Default.aspx.
10. From the **Trust the following certificate** drop-down menu, select the certificate you want. This should be the certificate from the **Certificate (Download Certificate)** of the **Application Created** page.

    ⓘ **NOTE:** You must first download and install the certificate you want before it can appear in this drop-down menu. See Downloading a Certificate for instructions on how to do this.
11. (Optional) Select the **Sign *AuthnRequest* message using this certificate** if you want it, and then select the appropriate certificate.
12. Click **Save**.

Adding the SMA Application to One Identity Cloud Access Manager

After you configure One Identity Cloud Access Manager (CAM) as an SMA Authentication Server, you need to add the SMA application to the One Identity CAM.

To add the SMA application to One Identity CAM:

1. In One Identity CAM, go to the Home page.
2. Under **Applications**, click **Add New**. The **Create a New Application** page displays.
3. Under **Create a New Application**, select **Configure Manually**. The **Back-end SSO Method** page displays.
4. Under **Back-end SSO Method**, select **Using SAML**.
5. Click **Next**. The **Federation Settings** page displays.
6. Under **Federation Settings**, enter the following URLs:
   a. In the **Recipient** field, enter `https://appliance.company.com/saml2ssoconsumer`.
   b. In the **Audience/SP Identity** field, enter `https://appliance.company.com`.
7. Click **Next**. The **Subject Mapping** page displays.
8. Under **Subject Mapping**, leave the default option selected, **Users from “AD” can’t log into this application**.

9. Click **Next**. The **Claims Mapping page** displays.
10. Leave the **Claim Mapping** section empty.
11. Click **Next**. The **External Access** page displays.
12. Under **External Access**, select **This application is external to my network**.
13. Click **Next**. The **Permissions** page displays.
14. On the **Permissions** page, select the **Roles** you want, using the **Allow Role Access** button.
15. Click **Next**. The **Application Name page displays**.
16. In the **Application Name** field, enter the name of your SMA application.
17. Click **Next**. The **Application Portal page** displays.
18. On the **Application Portal** page, under **SSO Mode**, select **SP Initiated**.
19. In the **URL** field, enter `https://appliance.company.com`.
20. Select any other options you want.
21. Click **Finish**. The **Application Created** page displays.

    The **Application Created** page shows all the Single Sign-On details necessary to configure the SMA application.

OneLogin

This section describes how to configure OneLogin as an SMA Authentication Server and how to add the SMA application to the OneLogin service.

Topics:

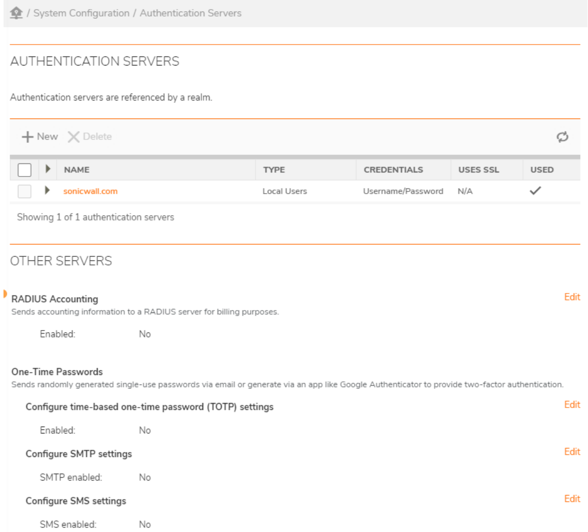
- Configuring OneLogin as an SMA Authentication Server
- Adding the SMA Application to OneLogin

Configuring OneLogin as an SMA Authentication Server

Configuring OneLogin as an SAML Identity Provider is done by configuring a OneLogin Authentication server on an SMA appliance.

To configure OneLogin as an SMA Authentication Server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

□	NAME	TYPE	CREDENTIALS	USES SSL	USED
□	sonicwall.com	Local Users	Username/Password	N/A	✓

Showing 1 of 1 authentication servers

OTHER SERVERS

RADIUS Accounting
Sends accounting information to a RADIUS server for billing purposes.

Enabled:	No

One-Time Passwords
Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings

Enabled:	No

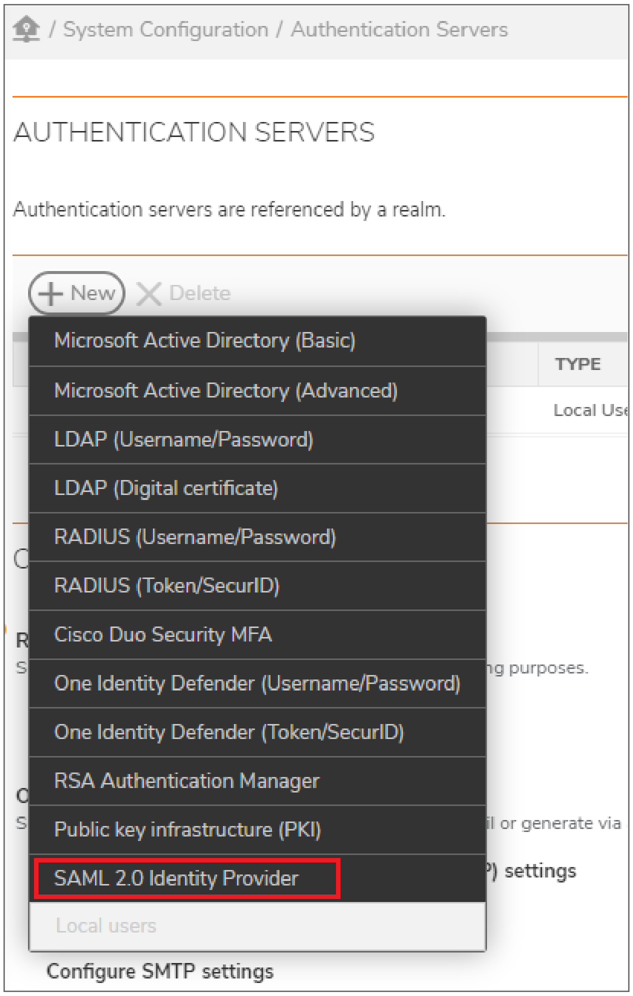
Configure SMTP settings

SMTP enabled:	No

Configure SMS settings

SMS enabled:	No

2. Under **Authentication servers**, click the **+** (New) icon. The **Add Authentication Server** page displays.



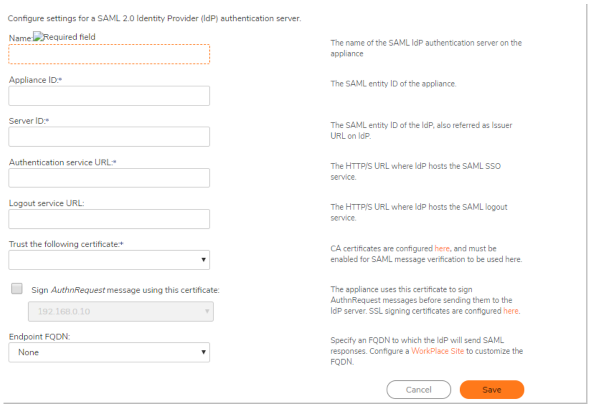
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
TYPE
Local Use
ng purposes.
il or generate via
) settings
Configure SMTP settings

3. Select **SAML 2.0 Identity Provider**.
4. Click **Continue....** The **Edit Authentication Server** page displays.



Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name: Required field — The name of the SAML IdP authentication server on the appliance

Appliance ID:* — The SAML entity ID of the appliance.

Server ID:* — The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:* — The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL: — The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:* — CA certificates are configured here, and must be enabled for SAML message verification to be used here.

□ Sign *AuthnRequest* message using this certificate: 192.168.0.10 — The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN: None — Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

The steps that follow explain how to configure the fields in the **Configure Authentication Server** .

5. In the **Name** field, enter **OneLogin_IDP**.
6. In the **Appliance ID** field, enter the **Audience/SP Identity** from the **Configuration** tab of the **SonicWall VPN** page. For example, `https://appliance.company.com`.
7. In the **Server ID** field, enter the **Issuer URL** from the **Configuration** tab of the **SonicWall VPN** page. For example, `https://app.onelogin.com/saml/metadata/xxxx`.
8. In the **Authentication service URL** field, enter the **IDP Login URL** from the **SSO** tab of the **SonicWall VPN** page. For example,

   `https://company.onelogin.com/trust/saml2/http-post/sso/xxxx`.
9. In the **Logout service URL** field, enter the **SLO Endpoint (HTTP)** from the **SSO** tab of the **SonicWall VPN** page. For example,

   `https://company.onelogin.com/trust/saml2/http-redirect/slo/xxxx`.
10. From the **Trust the following certificate** drop-down menu, select the **X.509 Certificate**.

    ⓘ **NOTE:** You must first download and install this certificate before it can appear in this drop-down menu. See Downloading a Certificate for instructions on how to do this.
11. (Optional) Select the **Sign *AuthnRequest* message using this certificate** if you want it, then select the appropriate certificate.
12. Click **Save**.

Adding the SMA Application to OneLogin

After you configure OneLogin as an SMA Authentication Server, you need to add the SMA application to the One Login service.

To add the SMA application to the OneLogin service:

1. In OneLogin, go to the **Home** page. The **Find Applications** page displays.
2. Under **Find Applications**, enter **sonicwall** in the search field and hit enter. The **Add Sonicwall VPN** page displays.
3. In the **Portal** panel, in the **Display Name** field, enter **SonicWall VPN**.
4. In the **Connectors** panel, for the **Connector Version**, select **SAML 2.0**.
5. Click **Save**. The **Sonicwall VPN** page displays.
6. Click the **Configuration** tab.
7. In the **Appliance** field, enter the FQDN for your appliance. For example,

   `https://appliance.company.com`.
8. Click the **SSO** tab.
9. In the **Enable SAML 2.0** panel, under the **X.509 Certificate** field, click **View Details**. The **Standard Strength Certificate** page displays.
10. Click the **Download** button to upload the CA Certificate to the SMA appliance.

Ping Identity PingOne

This section describes how to configure Ping Identity PingOne as an SMA Authentication Server and how to add the SMA application to the Ping Identity PingOne service.

Topics:

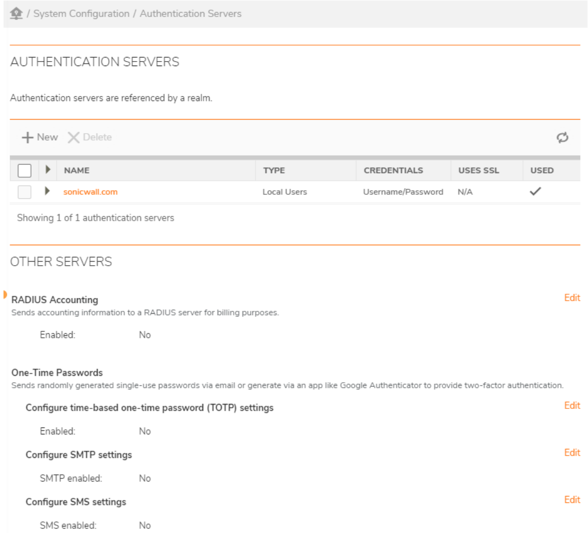
- Configuring Ping Identity PingOne as an SMA Authentication Server
- Adding the SMA Application to Ping Identity PingOne

Configuring Ping Identity PingOne as an SMA Authentication Server

Configuring Ping Identity PingOne as an SAML Identity Provider is done by configuring a Ping Identity PingOne Authentication server on an SMA appliance.

To configure Ping Identity PingOne as an SMA Authentication Server:

1. On the SMA appliance, go to the **System Configuration > Authentication Servers** page.



/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

□		NAME	TYPE	CREDENTIALS	USES SSL	USED
□		sonicwall.com	Local Users	Username/Password	N/A	✓

Showing 1 of 1 authentication servers

OTHER SERVERS

RADIUS Accounting

Sends accounting information to a RADIUS server for billing purposes.

Enabled: No

One-Time Passwords

Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings

Enabled: No

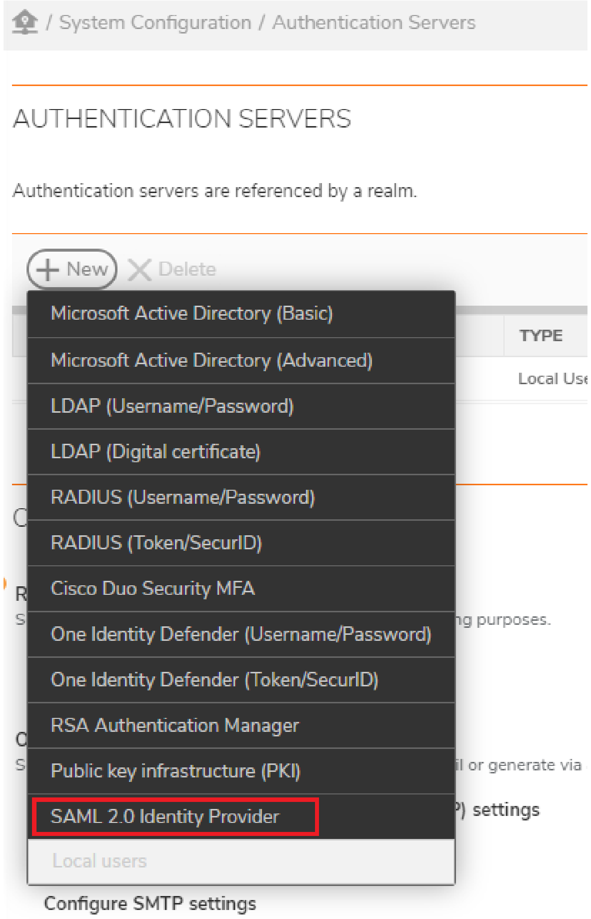
Configure SMTP settings

SMTP enabled: No

Configure SMS settings

SMS enabled: No

2. In the **Authentication servers** section, click the **+** (New) icon. The **Add Authentication Server** page displays.



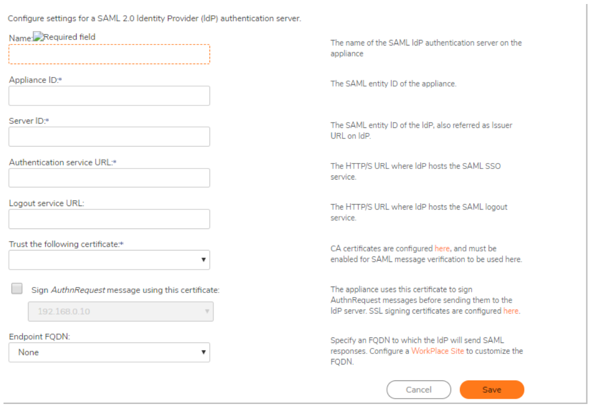
/ System Configuration / Authentication Servers

AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
TYPE
Local Use
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
ng purposes.
il or generate via
P) settings
Configure SMTP settings

3. Select **SAML 2.0 Identity Provider**.
4. Click **Continue....** The **Edit Authentication Server** page displays.



Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name: Required field — The name of the SAML IdP authentication server on the appliance

Appliance ID:* — The SAML entity ID of the appliance.

Server ID:* — The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:* — The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL: — The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:* — CA certificates are configured here, and must be enabled for SAML message verification to be used here.

□ Sign *AuthnRequest* message using this certificate: 192.168.0.10 — The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN: None — Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

Most of the values for the fields on this page can be obtained from the fields on the PingOne application page.

The steps that follow explain how to configure the fields in the **Configure Authentication Server** .

5. In the **Name** field, enter **PingOne_IDP**.
6. In the **Appliance ID** field, enter the **entityId** from the **PingOne** application page. For example: `https://appliance.company.com`.
7. In the **Server ID** field, enter the value of the **entityID** of the **EntityDescriptor** tag from the downloaded XML file, for example, `https://pingone.com/idp/company`.
8. In the **Authentication service URL** field, enter the **Initiate Single Sign-On (SSO) URL** from the **PingOne** application page. For example,

   `https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=734b784f-xx xxxx`.
9. In the **Logout service URL** field, enter the value of the **Logout Service URL** from the **Location** attribute of **SingleLogoutService** tag from the downloaded XML file. For example, `https://sso.connect.pingidentity.com/sso/SLO.saml2`.
10. From the **Trust the following certificate** drop-down menu, select the certificate you want. This should be the **Certificate** downloaded from the **PingOne** application page.

    > **NOTE:** You must first download and install the certificate you want before it can appear in this drop-down menu. See Downloading a Certificate for instructions on how to do this.
11. (Optional) Select the **Sign *AuthnRequest* message using this certificate** if you want it, then select the certificate.
12. Click **Save**.

Adding the SMA Application to Ping Identity PingOne

After you configure Ping Identity PingOne as an SMA Authentication Server, you need to add the SMA application to the Ping Identity PingOne service.

To add the SMA application to the Ping Identity PingOne service:

1. In PingOne, go to the **My Applications** page.
2. Under **Add Application**, select **New SAML Application**. The **Applications Details** panel opens.
3. Enter the **Application Name**.
4. Enter the **Application Description**.
5. Select the **Category** you want.
6. For **Graphics**, select the **Application Logo** and **Application** Icon you want.
7. Click **Continue to Next Step**. The **Application Configuration** panel opens.
8. For the **Protocol Version**, select **SAML v2.0**.
9. In the **Assertion Consumer Service (ACS)** field, enter the URL:

   `https://appliance.company.com/saml2ssoconsumer`.
10. Enter the **Entity ID**.
11. Enter the Application URL. This should be the same as appliance URL. For example,

    `https://appliance.company.com`.

12. For the **Single Logout Binding** Type, select **Post.**
13. Click **Next**. The **SSO Attribute Mapping** panel opens.
14. In the **Status** column, click in the row for the application to make it active.
15. Click **Save & Publish**
16. Click **Add new attribute.** The following panel opens.
17. To upload the CA Certificate to AMC, click Certificate **Download**.
18. Click SAML Metadata **Download**.
19. Click **Finish**.

Salesforce

This section describes how to configure Salesforce as an SMA Authentication Server and how to add the SMA application to the Salesforce service.

Topics:

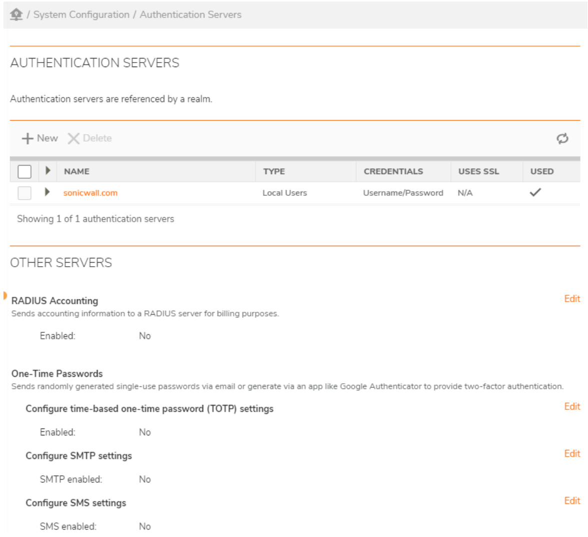
- Configuring Salesforce as an SMA Authentication Server
- Adding the SMA Application to Salesforce

Configuring Salesforce as an SMA Authentication Server

This section describes how to configure Salesforce as an SMA Authentication Server.

To configure Salesforce as an SMA Authentication Server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.



AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

□	NAME	TYPE	CREDENTIALS	USES SSL	USED
□	sonicwall.com	Local Users	Username/Password	N/A	✓

Showing 1 of 1 authentication servers

OTHER SERVERS

RADIUS Accounting
Sends accounting information to a RADIUS server for billing purposes.
Enabled: No

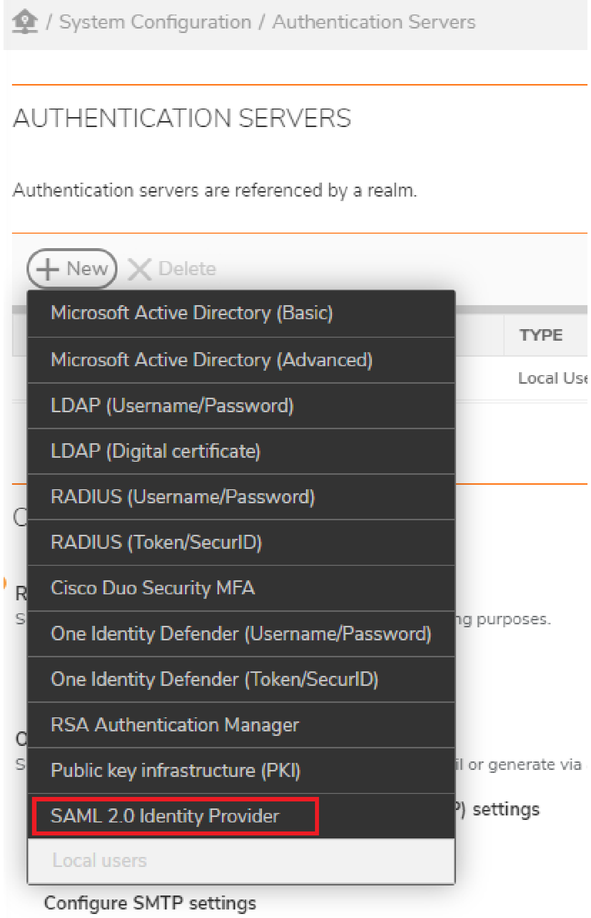
One-Time Passwords
Sends randomly generated single-use passwords via email or generate via an app like Google Authenticator to provide two-factor authentication.

Configure time-based one-time password (TOTP) settings
Enabled: No

Configure SMTP settings
SMTP enabled: No

Configure SMS settings
SMS enabled: No

2. In the **Authentication servers** section, click the **+** (New) icon. The **Add Authentication Server** page displays.



/ System Configuration / Authentication Servers

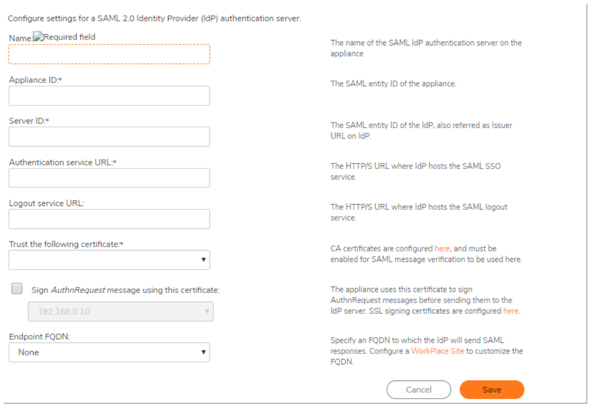
AUTHENTICATION SERVERS

Authentication servers are referenced by a realm.

New
Delete
Microsoft Active Directory (Basic)
Microsoft Active Directory (Advanced)
LDAP (Username/Password)
LDAP (Digital certificate)
RADIUS (Username/Password)
RADIUS (Token/SecurID)
Cisco Duo Security MFA
One Identity Defender (Username/Password)
One Identity Defender (Token/SecurID)
RSA Authentication Manager
Public key infrastructure (PKI)
SAML 2.0 Identity Provider
Local users
TYPE
Local Use
g purposes.
il or generate via
) settings
Configure SMTP settings

3. Select **SAML 2.0 Identity Provider**.

4. Click **Continue....** The **Edit Authentication Server** page displays.



Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name:Required field — The name of the SAML IdP authentication server on the appliance

Appliance ID:* — The SAML entity ID of the appliance.

Server ID:* — The SAML entity ID of the IdP, also referred as Issuer URL on IdP.

Authentication service URL:* — The HTTP/S URL where IdP hosts the SAML SSO service.

Logout service URL: — The HTTP/S URL where IdP hosts the SAML logout service.

Trust the following certificate:* — CA certificates are configured here, and must be enabled for SAML message verification to be used here.

□ Sign *AuthnRequest* message using this certificate: 192.168.0.10 — The appliance uses this certificate to sign AuthnRequest messages before sending them to the IdP server. SSL signing certificates are configured here.

Endpoint FQDN: None — Specify an FQDN to which the IdP will send SAML responses. Configure a WorkPlace Site to customize the FQDN.

5. In the **Name** field, enter **Saleforce_IDP**.

6. In the **Appliance ID** field, enter the **Entity Id** under **Web App Settings** from the **Salesforce** application page. For example, `https://application.company.com`.
7. In the **Server ID** field, enter the **Issuer** from the **Salesforce** application page, under **Web App Settings**. For example, `https://company.my.salesforce.com` as per application configuration in Salesforce.
8. In the **Authentication service URL** field, enter the **IdP-Initiated Login URL** from the **Salesforce** application page. For example,

   `https://company.my.salesforce.com/idp/endpoint/HttpRedirect`.
9. From the **Trust the following certificate** drop-down menu, select the certificate you want. This should be the certificate downloaded from the **Identity Provider** page.

   ⓘ **NOTE:** You must first download and install this certificate before it can appear in this drop-down menu. See Downloading a Certificate for instructions on how to do this.
10. (Optional) Select the **Sign *AuthnRequest* message using this certificate** if you want it, then enter the IP address for the certificate.
11. Click **Save**.

Adding the SMA Application to Salesforce

After you configure Salesforce as an SMA Authentication Server, you need to add the SMA application to the Salesforce service.

To add the SMA application to the Salesforce service:

1. Login to Salesforce.
2. Go to the **App Setup > Create > Apps > Connected Apps Detail** page.
3. Click **Add**. The **Settings** page displays.
4. In the **Web App Settings** panel:
   a. For **Start URL**, enter `https://appliance.company.com`.
   b. Select **Enable SAML**.
   c. For **Entity ID**, enter the Workplace URL: `https://appliance.company.com`.
   d. For **ACS URL**, enter `https://appliance.company.com`.
   e. For **Subject Type**, select **Username**.
   f. For **Name ID Format**, enter

      `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
   g. For **Issuer**, enter `https://company.my.salesforce.com`.
5. Click **Save**.
6. On the **App Setup > Create > Apps > Connected Apps Detail** page, click **Manage Profiles**.
7. Select the types of users you want to allow to access the Salesforce application.
8. Click **Save**. You can view the configured Sale force settings on the **SonicWall SMA** page.

Log File Output Formats

About Log Files

The SMA appliance records system and user events in a series of log files. You can view the log files in AMC or by sending the messages to an external syslog server—this process is described in System Logging and Monitoring. This section explains how to manually review log files from the command-line interface on the appliance itself and interpret the data.

File Locations

the Log file names for SMA services table lists the names of the log files on the appliance, which are initially stored locally (`/var/log/aventail/`).

Log File Names For SMA Services

Secure Mobile Access service	File format	File name
System messages Contains message logs for the Web proxy service, the network tunnel service, and the policy server. Unregistered device messages are also in this log. See System Message Log.	syslog	`access_servers.log`
Network tunnel service Includes information about connection activity, a list of users accessing the network, and the amount of data transferred for the network tunnel service. See Network Tunnel Audit Log.	SOCKS5LF	`extranet_access.log`

Web proxy service SeeWeb Proxy Audit Log.	W3C CLF	extraweb_access.log
Appliance Management Console (AMC) See Management Console Audit Log	syslog	policy_audit.log management.log
Client installation See Client Installation Logs (Windows).	syslog	<*username*>@<*realm*>.log
WorkPlace See WorkPlace Logs.	syslog	workplace.log wp_init.log
Upgrade log This log is a record of any upgrades you have made to the appliance.	text	upgrade.log
Migration log Stored in /var/log/, these are the logging messages recorded during migration from version <*n.n.n*>.	syslog	migrate_<*n.n.n*>.log

To minimize storage requirements for log files, the appliance rotates the files. The log rotation procedures vary, depending on the frequency you specify:

Log Rotation Procedures

Frequency	Procedure
Every 15 minutes	• Rotate any log files that are larger than 750MB. • Force a rotation of the syslog log file. • Turn on Compression for rotated files. • Compression Ratio is set to 0.10 of actual file size. • Each file is compressed after rotation.
Every day	• Force a rotation of all log files. • Delete any log files that are older than seven days.

Log files of more than one day old are stored in uncompressed format. The log file names contain a suffix that is numbered sequentially from 1 through 7, so that if the log rotation occurs daily, a log file with the suffix 7 is one week old. For example:

- `extraweb_access.log` is the current log file for Web proxy service.
- `extraweb_access.log1` through `extraweb_access.log.7` are the logs from the previous rotations.

System Message Log

The system message log (`/var/log/aventail/access_servers.log`) is generated in syslog format (see *RFC 3164*) and contains message logs for the Web proxy service, the network tunnel service, and the policy server (an internal service that controls policy for the other services). It also provides detailed messages about all access control decisions: each time a user request matches a policy rule, a log file entry is recorded explaining the action taken.

This sample message log entry is followed by descriptions of its elements:

```
[08/Nov/2016:07:16:24.312477 +0000] E-Class SMASSLVPN 002764 up 00000001 Info System CFG

Pool Init STATIC/NAT id=1 name='HQ-pool2' gid='AV1160554493976A' ndns=2 nwins=2 nsuffix=0
```

System Message Log Fields

Field	Description
`[08/Nov/2016:07:16:24.312477 +0000]`	
Precise timestamp	This timestamp indicates when the message was generated by the service (Web proxy, network tunnel, network proxy, or policy). This is a more accurate timestamp than the one generated by syslog because the logging system buffers messages before sending them to syslog.
`E-Class SMASSLVPN`	
Appliance name	This name can be changed on the Network Settings page in AMC (on the **Configure Basic Network Settings** page).
`002764`	
Process ID (PID)	Every application that is running is assigned a process ID. This PID identifies the application that generated the log entry.

`up`	
Application ID	Identifies the server process that generated the message. The possible IDs are: • `ap` (API server) • `cp` (SMA distributed cache client: policy server, client credential storage) • `dc` (SMA distributed cache server: policy server, client credential storage) • `ev` (network tunnel service—kernel component) • `ew` (Web proxy service) • `fm` (failover monitor) • `kp` (network tunnel kernel mode policy server interface) • `ks` (network tunnel kernel mode interface to SSL daemon) • `kt` (kernel tunnel component) • `ls` (log server) • `ps` (policy service) (Also see Access Policy Decisions) • `pt` (ping/traceroute tools) • `uk` (unknown) • `up` (network tunnel policy server daemon) • `us` (network tunnel user space SSL daemon)
`00000001`	
Context ID	The context ID is a unique value used to tie related logs from all four services (Web proxy, network tunnel, network proxy, policy, and WorkPlace) together. You can use the context ID to search for all messages related to a single user session. If a message is not tied to a particular user session, it is assigned a number lower than `00000010`. The first digit of this ID indicates which service originally generated the session: • `0` (policy service) • `1` (Web proxy service) • `3` (WorkPlace service)

`Info`	
Severity	The message severity levels are: • **Error**—A problem caused the server to shut down or fail to communicate with another component. A name resolution problem at startup is logged at this level. • **Warning**—Something unexpected occurred that does not adversely affect the operation of the server. For example, a single failed attempt to access a RADIUS server is logged at the Info level, but if all attempts fail, an entry is added to the log file at the Warning level. • **Info**—A normal event that you might want to track; for example, a specific user has logged in, or has matched a given access control rule. • **Verbose**—Like an Info message, this level identifies normal operations, but includes the steps in a process. For example, when processing access control rules a message for each non-match is at the Verbose level, while a matched rule is identified as Info.
`System`	
Message type	Indicates what part of the server logged the message.
`CFG Pool Init STATIC/NAT id=1 name='HQ-pool2' gid='AV1160554493976A' ndns=2 nwins=2 nsuffix=0`	
Message text	The text following all the identifying information is the message itself. See Access Policy Decisions for an explanation of the message text for access policy decisions.

Topics:

- Access Policy Decisions
- Viewing Client Certificate Errors in the Log
- End Point Control Interrogation
- Unregistered Device Log Messages

Access Policy Decisions

One of the main uses for the system message log is to audit access policy **decisions**. Each time a user request matches a policy rule, the appliance writes an entry to the message text field (the last field in the message log) explaining the action taken.

A sample message for an access policy decision looks like this:

```
[09/Nov/2016:02:45:32.282637 +0000] E-Class SMASSLVPN 002421 ps 100004b3 Info EWACL User '
(192.168.136.70 (Dominique Daba)@(Students)' connecting from '192.168.136.70:37975' matched
 rule 'accessRule(AV1091719670706:preauth access rule)', access to '127.0.0.1:455' is
permitted.
```

For each connection request that matches a rule, a log message is generated at the Info level. Requests that don't match a rule are logged at the Verbose level, and when no rule match is found the request is logged at the Warning level.

For policy decisions, the logging message text field (everything after `Info` in the previous example) includes the information shown in the Logging message text fields table.

Logging Message Text Fields

Field	Description
`EWACL`	
Log type	The access policy being evaluated. The log types are: • `CSACL`—client/server access policy • `EWACL`—Web access policy • `WPACL`—WorkPlace access policy • `NEACL`—file system access policy (file shares accessed from the Network Explorer page in WorkPlace)
`User '(192.168.136.70 (Dominique Daba)@(Students)'`	
User name	The user making the request. If the appliance is configured to use multiple realms, the username will appear in the format `(user)@(realm)`.
`connecting from '192.168.136.70:37975'`	
Source of request	The address of the user making the request.
`matched rule 'accessRule(AV1091719670706:preauth access rule)'`	
Match status	Rule match status (either `Matched` or `No Match`) and the ID for the rule.
`access to '127.0.0.1:455' is permitted`	
Rule outcome	Details If the rule matched, this field will be empty. If the rule did not match, one of the following messages will appear: • Source Network is `<network>` • Date/time specification <*time*> • User <*username*> not in User/Group List • Destination network is <*dest*> • Virtual Host is <*vhost*> • Destination services dest is <*dest*> • Command is <*command*> • UDPEncrypt is <*true or false*> • Key Length <*length from the policy rule*> requires a stronger cipher

If no rule matched, an Info-level message is generated indicating that no matching rule was found.

Examples

Example 1: Success at Info Level

```
[09/Nov/2016:02:45:32.712860 +0000] E-Class SMASSLVPN 002421 ps 10000531 Info Session
Authentication for user '(192.168.136.70 (Guest))@(Students)' SUCCESS for realm 'Visitors'
```

Example 2: Failure at Info Level

```
[09/Nov/2016:04:27:40.965127 +0000] E-Class SMASSLVPN 002873 ps 00000003 Info WPACL User '
(kevin figment)@(Students)' connecting from '192.168.136.70:0' found no matching access
rule, access to 'www.seattletimes.com:80' is denied.
```

Viewing Client Certificate Errors in the Log

If the appliance is unable to verify a certificate chain, a message such as this one appears in the system message log file:

```
[09/Nov/2016:21:28:14.610949 +0000] E-Class SMASSLVPN 001539 ps 10000042 Info System Auth:
CRL-CERT: Cert verification status = 0, err = 20 'unable to get local issuer certificate'
```

This message includes an error code (in this case, 20) reporting why the certificate check failed. These error codes are described in the Client certificate error codes table.

Client Certificate Error Codes

Code	Error message	Description
2	Unable to get issuer certificate	The issuer certificate of an untrusted certificate could not be found.
7	Certificate signature failure	The signature of the certificate is invalid.
9	Certificate is not yet valid	The certificate is not yet valid.
10	Certificate has expired	The certificate has expired.
18	Self-signed certificate	The passed certificate is self-signed and cannot be found in the list of trusted certificates.
19	Self-signed certificate in certificate chain	The certificate chain can be built using the untrusted certificates, but the root cannot be found locally.
20	Unable to get local issuer certificate	This normally means the list of trusted certificates is not complete. This error can also occur when an intermediate certificate is used for authentication (a root certificate is required).
21	Unable to verify the first certificate	No signatures could be verified because the chain contains only one certificate and is not self-signed.
22	Certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
23	Certificate revoked	The certificate has been revoked.

24	Invalid CA certificate	A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.

End Point Control Interrogation

The system message log captures information during client EPC interrogation when the log level is set to verbose. The appliance checks for the presence of certain device profile attributes on the client, and the log file records the query and the results.

In the following example, EPC is checking for a certain antimalware application (Symantec Client Security, version 9.x or later). When the application is not found, this particular device is relegated to the Default zone:

```
[04/Oct/2016:22:29:23.867093 +0000] E-Class SMASSLVPN 027186 uk 00000001 Verbose System
::API::QAABA145dFYNZimCKNWHB7p2q2Y=::(timwillis)@(Students)::CLIENT:: Interrogation:
Evaluation of OPSWATAV AV1128462569762A [NortonAV.dll,Symantec Corp.,Symantec Client
Security,>=,9.x,,,,,FALSE] results: FALSE
```

```
04/Oct/2016:22:29:23.875781 +0000] E-Class SMASSLVPN 027186 uk 00000001 Verbose System
::API::QAABA145dFYNZimCKNWHB7p2q2Y=::(timwillis)@(Students):: Classified into zone: Default
 zone
```

Unregistered Device Log Messages

Unregistered device log messages provide device IDs from login attempts by users on devices that are not registered. The AMC provides a way to export the unregistered device log messages in XML format. On the Logging page, select **Unregistered device log** from the **Log file** drop-down list and then click **Export**. You can reduce the size of the exported file by first applying filter or search criteria.

You can also access and export the list of unregistered devices to an XML format on another system. The list can be accessed directly in a Web browser using the following URL:

```
https://(internal IP address)/UnregisteredDevices.xml
```

This URL requires BASIC HTTP authentication, and the credentials must be an AMC user with at least View access to the Monitoring category.

A `curl` or `wget` command can be used to obtain the list programmatically from the external machine:

Command	Syntax
curl	`curl -k3u (user):(password) https://(internal IP):8443/UnregisteredDevices.xml`
wget	`wget --no-check-certificate --http-user=(user) --http-password=(password) https://(internal IP address):8443/UnregisteredDevices.xml`

Both of these commands turn off SSL certificate checking, which is useful when using a self-signed certificate.

A full definition of the URL used to fetch the XML version of the unregistered device report is provided in:

URL	*https://<internal address>:8443/UnregisteredDevices.xml?parameter=value&parameter=value*
Authentication	BASIC HTTP authentication, credentials must be AMC user with at least view access to the Monitoring category.
Parameters (all optional)	
username	string, case insensitive, default * (all users) Search for login attempts from users that contain this value as part of their username. Example: `username=li` will return entries for `Linda` and `Melinda`
realm	string, case insensitive, default * (all realms) Search for login attempts to Realms that contain this value as part of the Realm name. Example: `realm=Corp` will return entries for `Corporate` and `Non-Corporate`
platform	string, enumerated values below Search for login attempt from devices running only the specified platform: `all` — all platforms (default) `windows` —only Windows devices `mac` — only Mac devices `linux` — only Linux devices `activeSyncMobile` — only Exchange ActiveSync devices `mobilePhone` — only Mobile Phone devices `pda` — only PDA devices `unknown` — only devices on which the platform could not be determined
exported	string, enumerated values below Search for entries that have or have not already been exported either in AMC or via an HTTP get command. `all` — all entries, whether or not they have been exported (default) `exported` — only entries that have already been exported `unexported` — only entries that have not already been exported
limit	number, default 1000 Limit the search to this many entries.

deviceCount	number, 0-3, default all entries Search for users with only the specified number of devices already registered in the external AD/LDAP store. `0` — user has no devices registered `1` — user has one device registered `2` — user has two devices registered `3` — user has three or more devices registered
lastLoginTime	string, enumerated values below, default `all` Search for user login attempts that happened only in the time period specified, relative to the current time. `all` — all login attempts `hour` — attempts in the last hour `day` — attempts in the last day (24 hour period) `week` — attempts in the last week (7 days)

Network Tunnel Audit Log

The network tunnel audit log provides detailed information about connection activity, including the status of completed tunnel connections and the status of completed flows within tunnels.

ⓘ **NOTE:** The two record types can be distinguished by the word `flow` or `tunnel` appearing in the sixth field of the message.

Messages are stored on disk in the file `/var/log/aventail/extranet_access.log` and contain these parameters:

```
[source-ip:port] [authentication] "[username@realm]" "[date/time]" [version] [command]

[destination-ip:port] [status code] [bytes-received] [bytes-sent] [connection duration]
[imei]
```

This example illustrates a network tunnel service audit log file entry:

```
12.230.158.210:1110 ssl:LDAP "fred figment" "13/Sep/2016:19:18:28 -0700" v1.1 flow:tcp

192.168.136.254:22 0 21722 60631 263 490236207159217
```

The log entries contain the fields (separated by spaces) shown in the Network tunnel audit log fields table.

Network Tunnel Audit Log Fields

Field	Description

`source-ip:port`	For tunnel records this field contains the source address of the outer tunnel connection. For flows this field contains the inner flow source address, which is the virtual IP address assigned from a tunnel pool when the tunnel is established. Example:`12.230.158.210:1110`
`authentication`	A hyphen (-) indicates re-authentication via TEAM credential. ⓘ **NOTE:** An explicit value is not possible, because the tunnel does not know the authentication method used to negotiate the TEAM credential.
`"username@realm"`	User accessing the resource, and the realm he or she is logged in to. The format of this field varies, depending on the authentication method used. Example: "`mfigment@employees`"
`"date/time"`	Date (in date/month/year format) and time (hours, minutes, seconds, and milliseconds in 24-hour-clock format and hours of time zone +/- GMT) the connection began. ⓘ **NOTE:** Records containing date/time may not be written immediately to the log. Example: "`13/Sep/2016:19:18:28 -0700`"
`version`	The Connect or OnDemand Tunnel protocol version, with 1.1 for currently supported releases.

`command`	The type of command executed. These commands can appear in log file entries for the network tunnel service:
	`tunnel`
	`flow:tcp`
	`flow:udp`
	`flow:icmp`

`destination-ip:port`	IP address and port number of the resource being accessed. For flows, this is the destination of the TCP, UDP or ICMP flow. For tunnels, this is the external address of the appliance (port number is always 0). Example: `192.168.136.254:22`
`status code`	`0` is success. See Auditing Connection Status Messages for more detail about the status codes.
`bytes-received`	Number of bytes read from source.
`bytes-sent`	Number of bytes written to destination.
`connection duration`	Connection duration (in seconds) based on the time the tunnel was closed, a TCP flow entered its TIME_WAIT state, or a UDP or ICMP flow timed out.

imei	Every mobile phone is assigned a unique, 15-digit IMEI code (device identifier) that indicates information like the manufacturer, model type, and country of approval. The IMEI can be displayed on most phones by dialling `*#06#`. It's also shown on the compliance plate underneath the battery. Example: `352711-01-521146-5` If the IMEI code is not provided by the device, a platform identifier is shown. Platform identifiers (first character) are: W – Windows M – Mac L – Linux P – PDA A – AcitveSync Mobile X – Unknown (blank) – Mobile Phone

Auditing Connection Status Messages

The network proxy/tunnel audit log includes a connection status code that is often useful in debugging client/server connection problems. The status code is the field immediately following the destination-`ip:port` field in the log file (see Network Tunnel Audit Log for a description of an entire log file entry). the Connection status codes table describes each code.

Connection Status Codes

Connection status code	Description
0	Successful connection attempt with no errors encountered
1	Client presented an invalid TEAM credential
2	Couldn't send TEAM request to client, error in tunnel auth exchange, or error in PS auth exchange
3	Tunnel protocol at client is below minimum supported by appliance
4	TP error, or unsupported feature requested
5	Session sat idle longer than allowed by configuration or defaults
6	Tunnel pools have no addresses available
9	No tunnel internal address (bad cfg); realm_list (shouldn't happen) problem; client rejected resource list
10	Client version mismatch
11	All available tunnel pool addresses conflict with the client's networking environment in fatal ways
12	Special error to client indicating it should attempt a resume immediately

65535	Permission denied
65524	Out of memory
65520	System busy, session dropped
65514	Internal inconsistency, unexpected condition encountered
65504	Tunnel service aborted
65432	Connection reset by peer
65429	Not connected (internal error)
65428	Tunnel service shutdown
65426	Timeout (not necessarily an error, esp. for UDP flows)
65279	No authentication method
65278	Authentication failed (for example, the user entered an invalid username/password)
65277	Authentication I/O fail
65276	Authentication quiet fail
65275	Lost client connection
65274	Cannot load module
65273	Not authorized (for example, access denied due to policy)
65272	Encrypt failure
65271	Unknown failure

Examples

If a user enters an invalid username/password, error number 65535 appears in the log:

```
192.168.2.69:3127 ssl "testing" "26/Feb/2017:21:31:51.947 +0000" none -:- 65535 385 0 14
352711-01-521146-5
```

If a timeout occurred, the message contains error number 65426:

```
192.168.2.69:3127 ssl "testing" "26/Feb/2017:21:31:51.947 +0000" none -:- 65426 385 0 1
352711-01-521146-5
```

All tunnel traffic originating from the client and destined for the Internet (running in redirect-all mode) is routed through an IP address you specify on the **Configure Network Tunnel Service** page in AMC (**Enable route to Internet**). If this route to the Internet is not available, you'll see a connection status code of `65504`:

```
151.219.76.85:4827 - "(l248411)@(Radius)" "26/Jun/2016:17:54:14.916 +0000" 1.1 Flow:TCP
165.170.0.1:1503 65504 0 0 60 352711-01-521146-5
```

Web Proxy Audit Log

The Web proxy audit log provides detailed information about connection activity, including a list of users accessing your network and the amount of data transferred.

The `/var/log/aventail/extraweb_access.log` file messages are stored in the World Wide Web Consortium (W3C) Common Log Format (CLF). See http://httpd.apache.org/docs/logs.html for more information on CLF logs. The log message has these parameters:

```
[source-ip] [identity] [shortname@realm] [longname] [date/time] "[request]" [HTTP return
code] [bytes-sent] [imei]
```

The following is a sample network proxy/tunnel service audit log file entry:

```
192.168.200.162 - (extranetuser)@(Translation) (uid=extranetuser,ou=Users,dc=indigo,dc=com)
 [31/Mar/2017:09:08:09 -0700] "GET http:/
/127.0.0.1:455/postauth/interrogator/AventailComponents.exe HTTP/1.1" 200 536016 "-"
```

The log entries contain the fields (separated by spaces) shown in the Web Proxy audit log fields table.

Web Proxy Audit Log Fields

Field	Description
source-IP	IP address of the computer accessing the Web proxy service (this field may contain a translated address if NAT is in use). Example: `192.168.200.162`
identity	This field is not used by the Web proxy service; it always contain a dash (-).
shortname@realm	If the user has logged in, this field displays the user's name and login realm in the form (`username@realm`). If a user has not yet authenticated or is accessing content that does not require authentication (such as the WorkPlace login page), this field contains a dash (-). In cases where no authentication is used (that is, the **Authentication server** for the realm in AMC is set to **None**), this field will contain **anonymous-user**. Example: `(extranetuser)@(Translation)`
longname	If the user has logged in, this field displays the user's long name. LDAP and Active Directory usernames are displayed using a DN. Other usernames are display using a CN. If a user has not yet authenticated or is accessing content that does not require authentication (such as the WorkPlace login page), this field contains a dash (-). Example: `(uid=extranetuser,ou=Users,dc=indigo,dc=com)`

date/time	The date and time at which the request was received by the appliance. Example: `[16/Apr/2017:21:36:37 +0000]`
request	First line of the HTTP request, containing the HTTP command (such as `GET` or `POST`), the requested resource, and the HTTP version number. Example: `"GET /alias1/foo.gif HTTP/1.1"`
HTTP-return-code	The server responds with one of the following return codes: • `2xx` codes indicate a successful request. • `3xx` codes indicate some form of redirection or cached response. • `4xx` codes indicate an error (such as a resource that is not found or an unauthorized request). • `5xx` codes indicate a server error. For more information on these codes, see http://www.ietf.org/rfc/rfc2616.txt.
bytes-sent	Number of bytes sent in the body of the response (this does not include the size of the HTTP headers).
imei	Every mobile phone is assigned a unique, 15-digit IMEI code that indicates information like the manufacturer, model type, and country of approval. The IMEI can be displayed on most phones by dialling `*#06#`. It's also shown on the compliance plate underneath the battery. If there is no IMEI associated with the user, a dash (-) is entered in the log file. Example: `352711-01-521146-5`

Examples

- If an authentication attempt fails—for example, because the user enters an invalid username or password—a single message appears in the log with a return code of `200` (OK), indicating the client request was understood). Notice that the source IP address in the message is the only way for you to identify who made the request:

  ```
  192.168.2.69 - - [26/Feb/2017:21:43:30 +0000] "POST /__extraweb__authen HTTP/1.1" 200
  3610 352711-01-521146-5
  ```

  For a successful authentication, a similar message appears, but with a return code of `302` (Found). It is immediately followed by another message that contains the user's authentication credentials and a return code of `200`:

  ```
  192.168.2.69 - - [26/Feb/2017:21:44:25 +0000] "POST /__extraweb__authen HTTP/1.1" 302
  206 352711-01-521146-5
  ```

```
192.168.2.69 - (jsmith)@(AD) [26/Feb/2017:21:44:25 +0000] "GET /workplace/access/home
HTTP/1.1" 200 15424
```

- If a user successfully authenticates, but is denied access to a Web resource by an access rule, a message containing a return code of `403` (Forbidden) is logged:

  ```
  192.168.2.69 - (jsmith)@(AD) [26/Feb/2017:21:52:25 +0000] "GET /dukes HTTP/1.1" 403
  3358 352711-01-521146-5
  ```

- If a user successfully authenticates and is permitted to access a URL, a message appears that is identical to the one for a failed authentication (a return code of *200*), except that this one includes the user's credentials:

  ```
  192.168.2.69 - (jdoe)@(AD) [26/Feb/2017:21:51:03 +0000] "GET /dukes HTTP/1.1" 200 262
  352711-01-521146-5
  ```

Management Console Audit Log

An individual with administrative privileges can view a history of configuration changes that were made to the appliance by reviewing the AMC audit log. This log provides an audit history of configuration changes made in AMC by administrators. Follow the steps in Management Audit Log to view the log (`/var/log/aventail/policy_audit.log`) in AMC.

An additional AMC-related log file in syslog format (`/var/log/aventail/management.log`) is also available.

WorkPlace Logs

The WorkPlace log (`/var/log/aventail/workplace.log`) is useful for troubleshooting access to file shares using Network Explorer, and also answering questions about what Web and network shortcuts are shown on the WorkPlace portal page. Accessing file resources is also logged to the Web proxy service log (`extraweb_access.log`).

WorkPlace Shortcut Examples

When a user logs in to Workplace and successfully sees shortcuts, the log file entries looks like this:

1. The username credentials are logged with a session ID (when troubleshooting, just look for the username):

   ```
   Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,612] GOT:
   CredentialsManager[teamSessionId=+kMs+1fJYyVOxJ8f/YO0gg==,teamcredentials=
   {username=jdoe} ,credentials={}]
   ```

2. Later you see a message indicating a successful load of the shortcut (in this case a Web shortcut):

   ```
   Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,615] pcsession:
   <authorize:exit> uri=http://wemmet.internal.net status=SUCCESS
   ```

3. The successful load of a network shortcut looks like this:

```
Feb 26 22:03:03 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:03:03,617] pcsession:
<authorize:exit> uri=smb://marshare01/marketing status=SUCCESS
```

If a user does not see shortcuts (because of an access rule you have set up, for example), the denial of access looks like this:

1. Look for the username at login:

   ```
   Feb 26 22:12:15 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:12:15,027] GOT:
   CredentialsManager[teamSessionId=hZ98BEZxdyARJCtjkGl3lA==,teamcredentials=
   {username=dsmith} ,credentials={}]
   ```

2. Look for the shortcut information that is failing to load on the user's WorkPlace portal page. This is an example of a Web shortcut failure:

   ```
   Feb 26 22:12:15 127.0.0.1/127.0.0.1 local7.debug DEBUG [22:12:15,043] pcsession:
   <authorize:exit> uri=http://wemmet.internal.net status=FAILURE
   ```

ⓘ | **NOTE:**

- Access (permit/deny) to a resource share is also logged in `extaweb_access.log`:

  ```
  192.168.2.69 - (jdoe)@(AD) [26/Feb/2017:22:19:21 +0000] "GET
  /workplace/access/exec/file/view?path=smb://marshare01/marketing/ reports.doc/
  HTTP/1.1" 200 4608
  ```

- An additional WorkPlace-related log file in syslog format (`/var/log/aventail/wp_init.log)` is also available.

Internationalization Support

- Support for Native Character Sets
- RADIUS Policy Server Character Sets

Support for Native Character Sets

The appliance provides support for extended character sets or double-byte character sets so that usernames, passwords, resources, WorkPlace shortcuts, and access control rules can be entered and displayed in AMC using native character sets that contain extended or double-byte characters. This also allows support for extended characters or double-byte characters in user authentication prompts, such as username and password fields.

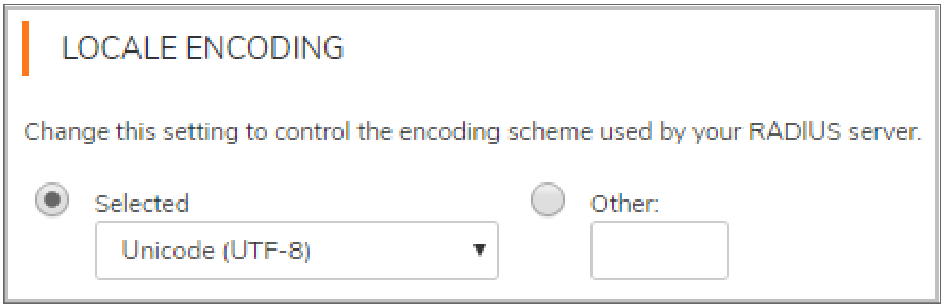
RADIUS Policy Server Character Sets

The appliance supports character encoding for RADIUS policy servers that use non-English character sets. The most recent version of the RADIUS specification (RFC2865) calls for all text fields to contain UTF-8 encoded characters. However, older versions of the RADIUS protocol define text fields as 7-bit US-ASCII. To support

RADIUS servers that use an older version of the protocol, AMC enables you to select from a list of the most commonly used character sets, and also lets you enter other character sets.

To change the language setting for a RADIUS server:

1. In the AMC, navigate to **System Configuration > Authentication Servers**.
2. In the **Other Servers** section, click **Edit** next to the RADIUS server you want to configure. (If you are configuring a RADIUS server in AMC for the first time, see Configuring RSA Server Authentication.)
3. On the **Configure Authentication Server** page, expand the **Advanced** area.
4. Under **Locale encoding**, do one of the following:



LOCALE ENCODING

Change this setting to control the encoding scheme used by your RADIUS server.

● Selected ○ Other:

Unicode (UTF-8) ▼

   - Choose a character set from the **Selected** list box (see Selected RADIUS Character Sets for the available character sets).
   - Click **Other**, and then type the name of a character set in the text box. See Other Supported RADIUS Character Sets for a list of those that can be entered.

5. Click **Save**.

Topics:

- Selected RADIUS Character Sets
- Other Supported RADIUS Character Sets

Selected RADIUS Character Sets

The character sets shown in are available from the **Selected** list (under **Advanced** settings) on the **Configure Authentication Server** page.

Selected RADIUS Character Sets

Character set	Code page
Arabic	1256
Baltic	1257
Central European	1250
Chinese Simplified (GBK)	936
Chinese Traditional (Big5)	950

Cyrillic	1251
Greek	1253
Hebrew	1255
Japanese (Shift-JIS)	932
Korean	949
Turkish	1254
Unicode (UTF-8)	65001
Vietnamese	1258
Western	1252

Other Supported RADIUS Character Sets

To set the encoding scheme used by your RADIUS server, type one of the character sets shown in the Other supported RADIUS character sets table in the **Locale encoding** area on the **Configure Authentication Server** page.

Other Supported RADIUS Character Sets

Language type	Supported character set		
European languages	ASCII	ISO-8859-10	MacRoman
	ISO-8859-1	ISO-8859-13	MacCentralEurope
	ISO-8859-2	ISO-8859-14	MacIceland
	ISO-8859-3	ISO-8859-15	MacCroatian
	ISO-8859-4	ISO-8859-16	MacRomania
	ISO-8859-5	KOI8-R	MacCyrillic
	ISO-8859-7	KOI8-U	MacUkraine
	ISO-8859-9	KOI8-RU	MacGreek
		CP850	MacTurkish
		CP866	MacOS
Semitic languages	ISO-8859-6	MacHebrew	
	ISO-8859-8	MacArabic	
	CP862		

Japanese	EUC-JP	
	ISO-2022-JP	
	ISO-2022-JP-2	
	ISO-2022-JP-1	
Chinese	EUC-CN	BIG5-HKSCS
	HZ	ISO-2022-CN
	GB18030	ISO-2022-CN-EXT
	EUC-TW	
	CP950	
Korean	CP949	
	ISO-2022-KR	
	JOHAB	
Armenian	ARMSCII-8	
Georgian	Georgian-Academy	
	Georgian-PS	
Tajik	KOI8-T	
Thai	TIS-620	
	CP874	
	MacThai	
Laotian	MuleLao-1	
	CP1133	
Vietnamese	VISCII	
	TCVN	
Unicode	UCS-2	UTF-16
	UCS-2BE	UTF-16BE
	UCS-2LE	UTF-16LE
	UCS-4	UTF-32
	UCS-4BE	UTF-32BE
	UCS-4LE	UTF-32LE
		UTF-7

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Secure Mobile Access for Administration Guide
Updated - February 2024
Software Version - 12.4.3
232-005698-00 Rev E

The information in this document is provided in connection with SonicWall and/or its affiliates’ products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/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