

Secure Mobile Access 12.4
Central Management Server
Administration Guide

SONICWALL®

Contents

About This Guide	4
CMS Configuration	4
GTO Configuration	5
Sonicwall Support	5
Guide Conventions	5
CMS Configuration	6
Introduction to CMS	6
Overview	7
CMS Deployment Options	8
What's New in This Release	9
Central Management Server	13
Central Management Console	14
Managed Appliances	15
Licensing CMS	15
Central User Licenses	16
Global Traffic Optimizer	16
FIPS and CMS	16
Getting Started in Five Steps	17
Installing and Configuring the Central Management Server	17
Overview	17
Kernel based Virtual Machine	18
Supported Platforms for CMS with Global HA	18
Hardware Resource Requirements	19
Installation Files	19
Setting Up a CMS	19
Configuring Appliances for Central Management	25
Overview	25
Firmware Compatibility with the CMS	25
Enabling Central Management on SMA Appliance	26
Registering an SMA Appliance with the CMS	29
Previously Configured Appliances	29
Using the Management Console Menus	29
Overview	30
Dashboard	30
Management Server	35
Managed Appliances	54
Central User Licensing	78

Overview	78
How Central User Licenses Work	78
Enabling Central User Licensing	81
Getting Started with Central User Licensing	81
Global High Availability	83
High Availability of the VPN Service	83
High Availability of the CMS	84
Disaster Recovery for the VPN Service	84
Alerts and SNMP	85
Overview	85
Pre-Configured Alerts	85
Configuring SNMP	86
Capture Advanced Threat Protection	87
Enabling Capture ATP	87
File Options	88
Web Services	90
Advanced Settings	90
Central FIPS Licensing	91
Global High Availability	92
Introduction to Global HA and GTO	92
CMS with GTO	94
Exchange ActiveSync and Outlook Anywhere	94
Custom FQDN for Mapped Resources	94
Viewing GTO Status from the CMS Console	95
GTO and IPv6	95
Deployment Notes	95
Planning GTO Deployment	96
Choosing a Deployment Model	96
Minimizing Configuration Differences	97
GTO Service Names and DNS Delegations	97
Provisioning Certificates	98
Setting up GTO	105
Setting up the CMS and SMA appliances	106
Enabling GTO service for managed appliances with the CMS	106
Setting up a Basic GTO Service	108
Monitoring and Configuring GTO	110
Defining the Central Policy	113
Extending GTO Deployment	113
Enabling Cached Credentials	114
Additional Deployment Notes	114
SonicWall Support	115
About This Document	116

About This Guide

This guide contains installation procedures and configuration guidelines for deploying the SonicWall® Central Management Server (CMS) with Global High Availability (Global HA) for Secure Mobile Access (SMA).

CMS Configuration

- [Introduction to CMS](#) describes the Central Management Server with Global High Availability and its features.
- [Installing and Configuring the Central Management Server](#) includes procedures for setting up and installing the CMS, setting up VPN appliances to be managed, defining the collection of managed appliances, and monitoring appliances from the CMS Dashboard.
- [Configuring Appliances for Central Management](#) includes information about configuring appliances for central management.
- [Using the Management Console Menus](#) explains the choices available with the CMS menus for operating and controlling the CMS and Managed Appliances. This includes information about Alerts, Configuration, Monitoring, and Maintenance.
- [Central User Licensing](#) includes information about the Central User Licensing (Pooled Licensing).
- [Global High Availability](#) describes the Always Online VPN service that is enabled for users when GTO is enabled.
- [Alerts and SNMP](#) contains information about how the CMS provides a new SNMP MIB that queries the CMS and managed appliances to get health and metrics data associated with the CMS as well as generating SNMP traps for critical alerts.
- [Capture Advanced Threat Protection](#) includes information about using the Capture ATP service to analyzes various types of content for malicious behavior.

GTO Configuration

- [Introduction to Global HA and GTO](#) provides overview information about CMS with GTO.
- [Planning GTO Deployment](#) describes how to configure the GTO service with CMS and ensure a highly available and optimized VPN infrastructure.
- [Setting up GTO](#) describes how to make deploying GTO easier by planning and adhering to a few guidelines.
- [Extending GTO Deployment](#) describes how to deploy and configure additional SMA appliances.

Sonicwall Support

- [SonicWall Support](#) includes Information about contacting technical support.

Guide Conventions

Convention	Use
Bold Text	Highlights field, button, and tab names. Also highlights window, dialog box, and screen names. Also used for file names and text or values you are being instructed to type into the interface.
<i>Italic Text</i>	Indicates the name of a technical manual, emphasis on certain words in a sentence, or the first instance of a significant term or concept. Italics text also represents a variable in an expression. It should be replaced with the real item, for example, a file name.
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, System > Status means select the Status page under the System menu.

CMS Configuration

Topics:

- [Introduction to CMS](#)
- [Installing and Configuring the Central Management Server](#)
- [Configuring Appliances for Central Management](#)
- [Using the Management Console Menus](#)
- [Central User Licensing](#)
- [Global High Availability](#)
- [Capture Advanced Threat Protection](#)
- [Alerts and SNMP](#)

Introduction to CMS

Topics:

- [Overview](#)
- [CMS Deployment Options](#)
- [What's New in This Release](#)
- [Central Management Server](#)
- [Central Management Console](#)
- [Managed Appliances](#)
- [Licensing CMS](#)
- [Central User Licenses](#)
- [Global Traffic Optimizer](#)
- [FIPS and CMS](#)
- [Getting Started in Five Steps](#)

Overview

This section is an introduction to the SonicWall™ Central Management Server (CMS) with Global High Availability (Global HA) and provides important concepts associated with it. CMS is an add-on product for managing multiple Secure Mobile Access (SMA) VPN appliances. It gives customers with multiple appliances a single administrative user interface from where they can manage all their VPN appliances. CMS is a virtual machine that interacts with the managed SMA appliances. CMS reduces the total cost of operation and simplifies the management of multiple VPN appliances for organizations.

Global HA enables SMA appliances to scale performance by deploying multiple appliances under the same service name (e.g. access.example.com). Global HA eliminates a single point of failure and provides resilience whether customers deploy 2 SMA appliances in the same data center or across multiple data centers around the globe. A distributed data store shares user session state and licensing information across the mesh network of SMA appliances in an active-active cluster. This allows for session persistence across data centers. In the event of a fail-over, users get connected to another appliance in the service. Their experience is frictionless and productivity is not impacted. The distributed data store also allows for central user licenses to be shared across appliances and data centers.

① **NOTE:** SMA appliances in the Global HA mesh must be able to communicate with each other via their external interface IP addresses, Internal interface IP addresses or Pool IP addresses to facilitate sharing of information in the distributed data store.

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.

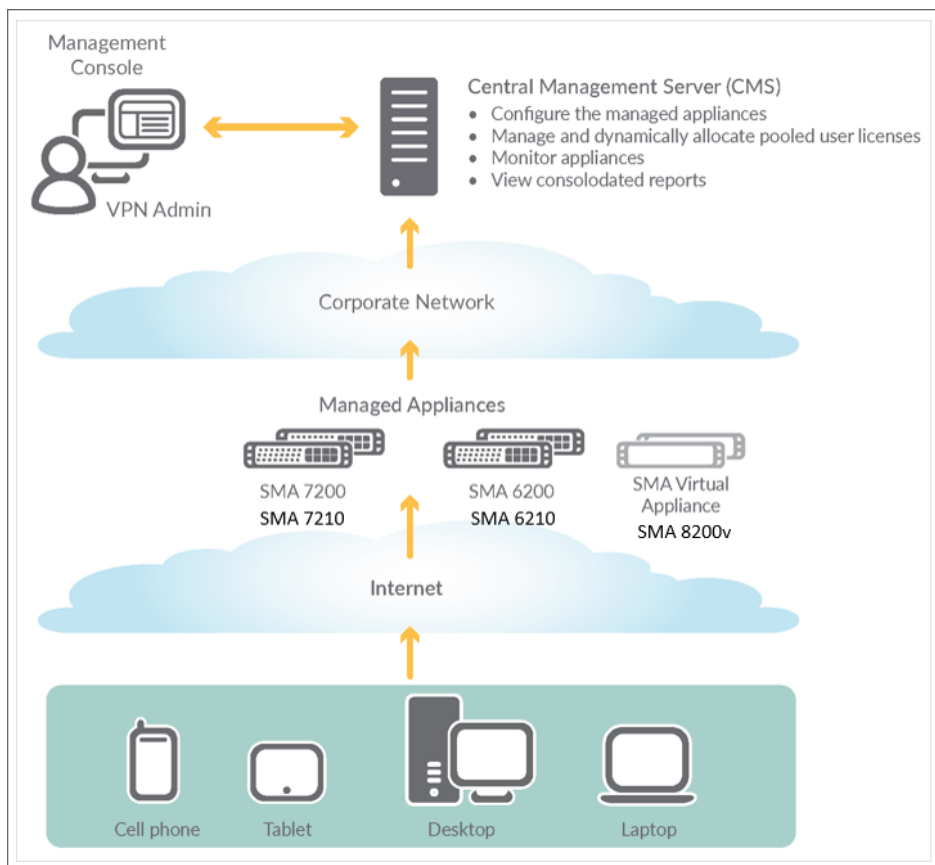
The CMS is a virtual machine, requiring no dedicated appliance or hardware, and provides the following features:

- A single dashboard for managing a distributed VPN infrastructure.
- Simplified license management with a centralized license that eliminates the need for separate appliance licenses. The license is shared by appliances.
- Central Management Console (CMC) to configure, maintain, and monitor appliances.
- Reduced Total Cost of Operation (TCO) of the VPN infrastructure.
- Reduced operator errors associated with managing multiple appliances that may be in different data centers.
- Centralized alerts via the console dashboard and SNMP traps.
- Global High Availability that is enabled with the Global Traffic Optimizer (GTO) service.

This dashboard view in the CMC gives the administrator a summarized view of all managed appliances.

Administrators 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.

An administrator can click on a single appliance in the CMC to launch the Appliance Management Console (AMC) for that appliance because of a single-sign on system.



CMS Deployment Options

Depending on your operational needs, CMS can be deployed in four phases:

- **Phase 1: Deploy CMS to only monitor and maintain standalone SMA appliances.**

This gives you a dashboard view and a single console from which to monitor and maintain all your SMA appliances.

- **Phase 2: Enable Central User Licenses on CMS.**

Central user licenses allows you to optimize user licenses across all your SMA appliances.

- **Phase 3: Use CMS to manage configurations.**

A centralized policy on the CMS, that is normalized across all your SMA appliances, simplifies configuration management, and gives users a consistent experience when they get connected to any appliance in your VPN infrastructure.

- **Phase 4: Enable Global High Availability using the Global Traffic Optimization Service.**

GTO provides a highly available VPN infrastructure where users connect to a single domain name (such as access.example.com) and get redirected to an available and proximate appliance.

① | **NOTE:** Central User Licensing and centralized policies are required for enabling GTO.

What's New in This Release

Version 12.4.3 of the Secure Mobile Access (SMA) Central Management Server (CMS) include these new features:

Topics:

- [Global Policy Settings](#)
- [CMS Alerts Logging](#)

Global Policy Settings

From 12.4.3 onwards, **Enabled** option is introduced in the Resource Groups and Exclusions.

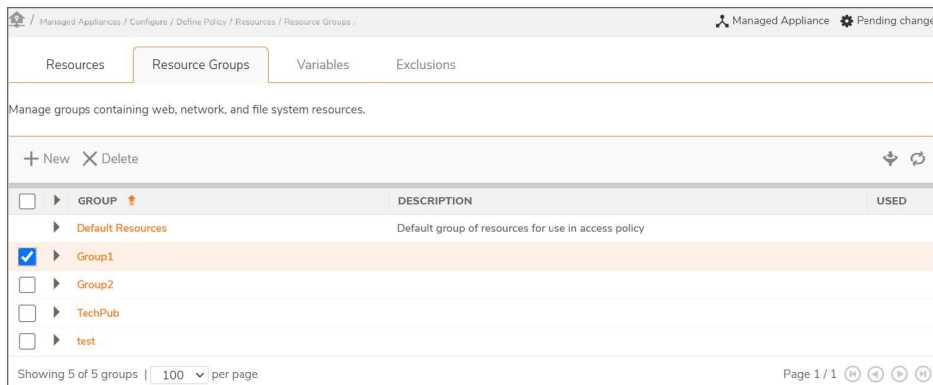
Prerequisites:

- CMS running 12.4 firmware version.

Configuring Global Policy Setting in Resource group

To configure global policy in resource group:

1. In the CMS, navigate to **Managed Appliances > Configure > Define Policy > Resources**.
2. Click the **Resource Groups** tab.



3. Click the **New** icon to add a resource group.

Home / Managed Appliances / Configure / Define Policy / Resources / Resource Groups / Add

Create or modify a resource group.

Name: * 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**.

+ Add X Remove

<input type="checkbox"/>	RESOURCE	DESCRIPTION
No rows to display		
Showing 0 of 0 resources		

GLOBAL POLICY

When using policy synchronization with the Global Traffic Optimizer service, all resource groups will be enabled on all managed appliances. You can optionally limit a resource group to be enabled only on certain appliances.

Enable this resource group on:

All appliances

IND1

IND2

IND3

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 allow the access to those created resource groups.
 - ① | **NOTE:** Disabled resource group does not allow or deny access.
7. Under **Global Policy**, select the appliances to include the resource group.
8. Click **Save**.

Configuring Global Policy Setting in Exclusions

To configure global policy in exclusion:

1. In the CMS, navigate to **Managed Appliances > Configure > Define Policy > Resources**.
2. Click the **Exclusions** tab.

Managed Appliances / Configure / Define Policy / Resources / Exclusions

Resources Resource Groups Variables **Exclusions**

Use this page to configure exclusions to prevent host names, IP addresses, subnets, IP ranges, or domains from being redirected to the appliance 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 rule for it.

+ New ✕ Delete

	ENABLED	NAME	DESCRIPTION
<input type="checkbox"/>	<input checked="" type="checkbox"/>	TechPub	Technical writing

Showing 1 of 1 exclusions

3. Click the **New** icon to add a resource group.

Managed Appliances / Configure / Define Policy / Resources / Exclusions / Add

Configure an exclusion to prevent a specific network resource from being redirected through the appliance.

Name: * Name this exclusion.

Description:

Enabled Disabled exclusions do not affect access policy

Values:

Each exclusion may contain up to 500 values.

GLOBAL POLICY

When using policy synchronization with the Global Traffic Optimizer service, all exclusions will be enabled on all managed appliances. You can optionally limit a exclusions to be enabled only on certain appliances.

Enable this exclusion on:

All appliances

IND1

IND2

IND3

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.

4. Enter the **Name** of the exclusion.
5. Enter the description for the exclusion if required.
6. Select the **Enabled** check box allow the access to those created exclusion.
 - ① | **NOTE:** Disabled exclusions do not does not exclude anything.
7. 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.
8. Under **Global Policy**, select the appliances to enable the exclusion.
9. Click **Save**.

CMS Alerts Logging

From 12.4.3 onwards, every action on Alerts will generate a log message in management message logs when it is triggered, acknowledged, and cleared. Similarly the alert creation, deletion or modification also will be logged under management audit logs.

Prerequisites:

- CMS running 12.4 firmware version.

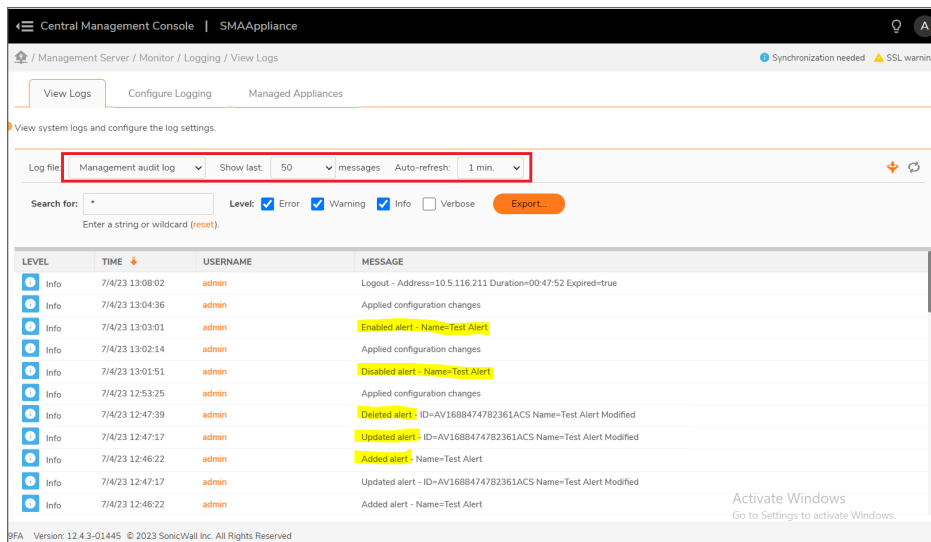
To View the CMS Alerts Logging :

1. In the CMS, navigate to **Managed Server > Monitor > Logging**.
2. Click the **Views logs** tab.
3. To view the Logs, select the **Management message log** or **Management audit log** from the drop-down in the **log file** field. Select the number of message from the **Show last messages** drop-down and auto-refreshed number of minutes from **Auto-refresh** drop-down.
4. The **Management message log** displays the details of alerts which contains information as follows:

LEVEL	TIME	SOURCE	MESSAGE
Info	7/5/23 15:52:03	AMC	Alert acknowledged, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=1, id=AV1689562609047AE, user=admin
Info	7/5/23 13:11:08	AMC	Alert acknowledged, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=0, id=AV1689562609047AE
Info	7/5/23 13:10:08	AMC	Alert cleared, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=25, id=AV1689562493104AD
Info	7/5/23 13:09:01	AMC	Alert activated, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=1, id=AV1689562493104AD
Info	7/5/23 13:04:09	AMC	Alert cleared, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=11, id=AV1689561888884AC
Info	7/5/23 12:59:08	AMC	Alert activated, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=8, id=AV1689561888884AC
Info	7/5/23 12:58:08	AMC	Alert cleared, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=25, id=AV1689561888884AB
Info	7/5/23 12:55:13	AMC	Alert activated, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=5, id=AV1689561888884AB
Info	7/5/23 12:53:08	AMC	Alert cleared, priority=CRITICAL, name=Test Alert, system=App06, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=12, id=AV168956129944AHK
Info	7/5/23 12:43:10	AMC	Alert activated, priority=CRITICAL, name=Test Alert, system=App07, metric=CPU_USAGE, condition=METRIC_UNDER_THRESHOLD, threshold=10, duration=0, value=0, id=AV1689569910161AA

- Event, system, priority, alert name, metric, condition, threshold, duration, measured metric value, username, and a unique ID.

- Type of alerts that are logged: Alerts acknowledged, alerts activated, alerts cleared.
5. The details of configuration of alerts are also logged under **Management audit logs**:



- Enabled alert, disabled alert, deleted alert, added alert, and updated alerts are viewed in the management audit log.

Central Management Server

CMS is only available as a virtual machine. Details about the supported platforms is listed in [Supported Platforms for CMS with Global HA](#).

CMS can manage up to 100 appliances (physical and virtual appliances), but before an appliance can be managed it must be registered with CMS. CMS registration is secured with encryption using a one time password. Its purpose is to bootstrap TLS communication by exchanging public keys. Following registration all CMS/appliance communication is secured with TLS.

The CMS communicates with each managed appliance to receive:

- Data on the Control channel for configuring, licensing, maintaining appliances.
- Periodic health and status information from managed appliances.

CMS periodically communicates with MySonicWall for license validation. This ensures correct system wide timing and use of licenses.

CMS also requires access to the following two online services:

	SonicWall Licensing Server	SonicWall Geo Server
FQDN	software.sonicwall.com	geows.global.sonicwall.com
Ports	443	443

- ① | **NOTE:** CMS must be able to communicate with each appliance on port 443 of one of the following IP addresses: the internal IP address, external IP address, or Pool IP address.
- ① | **NOTE:** Do not use more than one CMS for a single managed appliance.

Central Management Console

The Central Management Console (CMC) provides the user with a single screen (called the Dashboard) to show Active alerts, Appliance status, License status, and Geographic View of all appliances on a map of the world. The Dashboard also allows you, from a single point to:

- Configure appliances (using push configuration settings).
- Maintain appliances: Upgrade/hotfix, EPC update, add SSL certificates, and Restart.
- Use a one-click (single sign-on) to the AMC of managed appliance.
- View health history and reports for all appliances.
- Configure alerts, manage alert notifications for appliances or CMS.
- Install a central user license. Central licenses are available to all appliances as user demand changes between appliances.

Central Management Over the Internet

With Central Management Over the Internet, you can manage SMA appliances hosted in a data center using a CMS that is hosted outside the data center. You can also manage SMA appliances located in a different data center (without a dedicated link between the data centers) over the Internet.

Central Certificate Management

From the CMS, administrators can also manage certificates for all of the appliances managed by the CMS by:

- Creating and managing a Let's Encrypt free certificate.
- Creating Certificate Signing Requests, facilitating the process of obtaining certificates from a Certificate Authority.
- Importing certificates issued by a Certificate Authority to a centralized store on the CMS.
- Deploying selected certificates to specific appliances and then configuring those appliances to use the selected certificates, either immediately or at a scheduled time.
- Reviewing the list of certificates that have been imported to the CMS.
- Being alerted when certificates are due to expire.

Managed Appliances

Managed appliances are SMA 1000 series appliances that are registered with the CMS so that they can be centrally managed.

Each managed appliance must be an SMA Version 12.4 (or later) SMA appliance. A group of managed appliances may consist of physical and/or virtual appliances.

In this document, the term SMA 1000 series appliance refers to these appliances:

- SMA 6200
- SMA 6210
- SMA 7200
- SMA 7210
- SMA 8200v

Managed appliances send health and status information to the CMS. They accept policy configuration, user licenses, and maintenance commands from the CMS. Managed appliance communication with a CMS is secured with TLS.

① | **NOTE:** CMS must be able to communicate with appliances on port 443.

Licensing CMS

CMS has the ability to manage appliances licensed with different feature sets. Unlike SMA appliances, the CMS contacts the online SonicWall License Manager service to obtain its license.

① | **NOTE:** SMA appliances download and import a license file from the MySonicWall portal.

To license the CMS initially, you enter the serial number and authentication code into the CMS console. The CMS then contacts the License Manager service and obtains its license. After that, the CMS periodically contacts the License Manager service to refresh its license.

A CMS Base License is available at no cost from MySonicWall. You enable a CMS Base License by entering the serial number and the authentication code. A CMS Base License allows you to manage three appliances. A CMS Base license comes with a trial for pooled licenses for a limited period of time. A CMS Base License enables you to use the CMS without pooled licensing. A CMS Base License enables you to manage and monitor licensed SMA appliances. You can upgrade from a Trial License to a Base License.

Central User Licenses (Pooled Licenses) are shared licenses that are available to CMS-managed appliances. To use pooled licensing, you must add Central User Licenses to the CMS Base License. Central User Licenses can be subscription licenses (valid for specific periods of time, such as 1 year or 3 years), or perpetual licenses (without an expiration date).

Central User Licenses

CMS supports an optional pooled licensing model that allows user licenses to be centralized on the CMS and available to the managed appliances. Individual VPN appliances must have their own license before it can be joined to the CMS. Customers with appliances that are globally distributed can benefit from the fluctuating demands for user licenses due to time differences. Central user licenses are available to managed appliances where user demands have peaked when license demand has fallen in other regions due to off-work/night hours. For more information, refer to [Central User Licensing](#).

Global Traffic Optimizer

GTO allows customers to deploy a VPN infrastructure without the need for load balancers or global traffic management using a CMS and SMA 1000 series appliances. The SMA appliances may be located in a datacenter or globally distributed.

GTO allows customers to deploy the SonicWall GTO service. A GTO service is an online VPN service that is enabled by a cluster of SMA appliances working in concert to provide users with a highly available and optimized VPN infrastructure.

The GTO service distributes VPN connection requests from users to the appropriate SMA appliances. Load distribution is done using heuristics based on system parameters that are known and monitored by the GTO service. These parameters include appliance availability, appliance proximity to the user, user load, and appliance capacity.

① | **NOTE:** To use GTO with Connect Tunnel, Connect Tunnel must be upgraded to 12.1 or above.

FIPS and CMS

FIPS can be enabled on centrally managed appliances.

- A central FIPS license allows all appliances managed by the CMS to be FIPS-enabled.
- A CMS can obtain a central license (that includes FIPS) from:
 - The MySonicWall License Manager service
 - A central license file (for closed networks)
- To be managed by the CMS, FIPS-enabled appliances are not required to be part of a GTO service.
- A CMS license that includes FIPS must also include central user licenses. An appliance that is not centrally licensed cannot be FIPS-enabled from a CMS-based license.

When the CMS central user license has FIPS, the administrator can enable FIPS individually for any managed appliance from its AMC. (See “*Enabling FIPS*” in the *SMA 12.4 Administration Guide* for more information).

Getting Started in Five Steps

1. Install and configure the CMS and apply the CMS license.
Refer to [Installing and Configuring the Central Management Server](#).
2. Configure GTO.
Refer to [Setting up GTO](#).
3. Setup the VPN appliances to be managed.
Refer to [Configuring Appliances for Central Management](#).
4. Define the collection of managed appliances.
Refer to [Add/Remove](#).
5. Monitor and manage appliances from the CMS Dashboard.
Refer to [Dashboard](#).

① **NOTE:** When updating an SMA infrastructure that is already in place with upgrades and hotfixes, the managed SMA appliances are updated first, and then CMS is updated last.

Installing and Configuring the Central Management Server

Topics:

- [Overview](#)
- [Kernel based Virtual Machine](#)
- [Supported Platforms for CMS with Global HA](#)
- [Hardware Resource Requirements](#)
- [Installation Files](#)
- [Setting Up a CMS](#)

Overview

The Central Management Server with Global High Availability (CMS with GTO) is located inside a corporation's intranet. CMS requires a new type of license called a CMS License that is issued by SonicWall.

The CMS runs as a virtual machine that can be hosted on VMware ESX/ESXi, Microsoft Hyper-V, AWS, Azure, or KVM. CMS is not designed to run on custom hardware such as VPN appliances.

CMS with GTO provides the following features:

- Central Management Console (CMC) to monitor, maintain, and configure SMA appliances
- Simplified license management with a centralized license that eliminates the need for individual appliance licenses
- Centralized alerts via the console dashboard and SNMP traps
- Global Traffic Optimizer (GTO)

Kernel based Virtual Machine

SMA and CMS is enhanced to support KVM hypervisor. KVM, or Kernel based Virtual Machine is a software module that allows Linux to operate as a hypervisor. QEMU, or Quick Emulator, allows guest operating systems to run on the KVM hypervisor and supports virtualization where applications executing in the user space can achieve near native speeds through full virtualization or paravirtualization.

SMA supports the following hypervisors:

- VMware ESX
- Amazon EC2
- Microsoft Azure
- Microsoft HyperV
- QEMU + KVM

For more information on how to configure SMA on KVM, refer to the *SMA 12.4 KVM Getting Started Guide*.

Supported Platforms for CMS with Global HA

CMS with GTO runs as a virtual machine on these hypervisor platforms:

SUPPORTED PLATFORMS

VMWare	ESXi 6.x or higher
Microsoft Hyper-V	Windows Server 2016, Windows Server 2019
KVM	KVM version: 2.11.1
Cloud Platform	Azure and AWS

CMS with GTO is supported on the following SMA 1000 series appliances:

- SMA 6200
- SMA 6210
- SMA 7200
- SMA 7210
- SMA 8200v (ESXi/Hyper-V/AWS/Azure/KVM)

Hardware Resource Requirements

The virtual instance of CMS requires the following hardware resources:

- 8 GB RAM
- 4 CPU
- 250 GB (Storage Requirements)

Installation Files

The Central Management Server should run the same firmware version as the appliances it manages.

- To install on VMware hypervisors, the Open Virtualization Archive (.OVA) file with the following file name format is available for import and deployment to your ESX/ESXi server: `ex_sra_vm_12.x.x-xxx.ova`.
- To install in a Microsoft Hyper-V environment, use an International Organization for Standardization (.ISO) file such as: `12.x.x-xxx.iso` or Virtual Hard Disk (.vhd) file such as: `12.x.x-xxxx.vhd.tgz`.
- To install in a KVM environment, use an International Organization for Standardization (.ISO) file such as: `12.x.x-xxx.iso`.
- To get the SMA AMI for AWS and Azure:
Contact SonicWall Sales at <https://www.sonicwall.com/customers/contact-sales>
OR
SonicWall Support at <https://www.sonicwall.com/support/contact-support>

The 12.x.x indicates the SMA release version and xxx represent a build number.

① | **NOTE:** The same firmware is used for both the CMS and the SMA 8200v. The Central Management feature is enabled during the setup process.

For information on installing the CMS on AWS, Azure, and KVM, refer to the respective *SMA 12.4 Getting Started Guides*.

Setting Up a CMS

To setup a Centrally Managed VPN infrastructure:

① | **NOTE:** For setting up a CMS on AWS, Azure and KVM, refer to the respective *Getting Started Guide*.

1. Setup a virtual instance (ESX/ESXi, Hyper-V) of the release firmware.
2. Start the virtual machine and wait for a login prompt to appear.
3. Login as **root** (no password is required).
4. Press any key to continue.

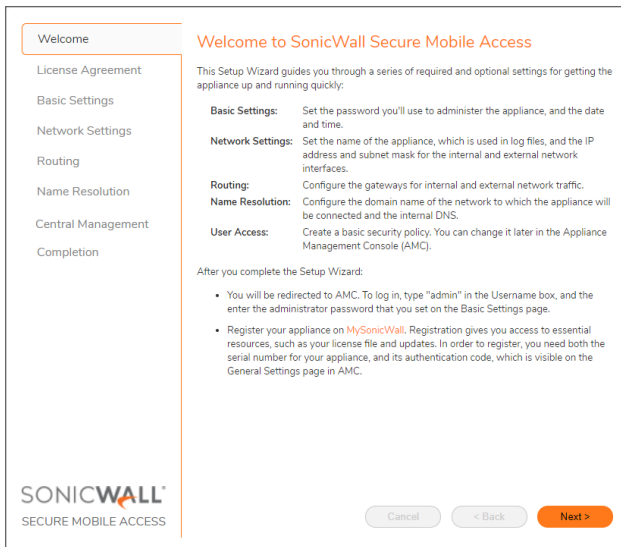
5. Enter the network settings for the internal interface (labeled 2 on the appliance).

- IP Address
- Subnet mask
- Gateway

① | **NOTE:** If you are on the same network as the appliance, press **Enter** when prompted for the gateway.

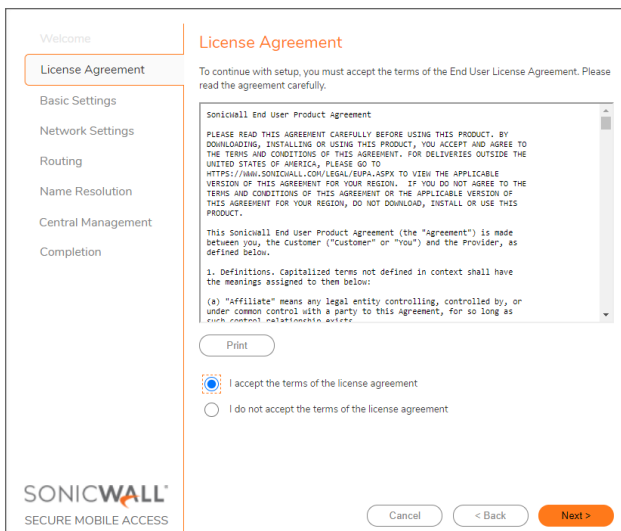
6. Continue the Setup Wizard steps to access the console from a browser at `https://<Internal-IP-Address>:8443`

The Setup Wizard **Welcome** screen displays.



7. Click **Next** to view the **License Agreement**.

8. Read the agreement and, if you agree, select **I accept the terms of the license agreement**.



9. Click **Next**.
The **Basic Settings** page displays.
10. Select **Configure this machine as a CMS to manage the licensing and configuration of up to 100 SMA appliances**.
11. Under **Administrator password**, enter the password you want for the administrator and confirm it.
 ⓘ | **IMPORTANT:** Be sure to save or write this password down in a secure location. If you forget it, it cannot be recovered.
12. Under **Date and time**, select the time zone from the **Time Zone** menu.

The screenshot shows the 'Basic Settings' page for 'Central Management'. On the left is a navigation menu with 'Basic Settings' selected. The main content area has the following sections:

- Central Management:** A heading followed by the text: 'This machine can be configured as a central management server (CMS) to manage the licensing and configuration of up to 100 SMA appliances.' Below this are two radio buttons: 'Configure this machine as an SMA appliance' (unselected) and 'Configure this machine as a CMS to manage the licensing and configuration of up to 100 SMA appliances' (selected).
- Warning:** An orange box with a warning icon and text: 'A CMS does not serve user connections. Its purpose is to manage SMAs'.
- Administrator password:** A heading followed by the text: 'Specify the password you will use to access the Appliance Management Console (AMC). Your password must be at least eight characters long.' Below this are two input fields: 'Enter password: *' and 'Confirm password: *'.
- Date and time:** A heading followed by the text: 'Please select a time zone below. To set the current time, click **Change**. If you wish to synchronize the time with an NTP server, it can be configured later in AMC.' Below this is a 'Time zone:' dropdown menu showing 'GMT+00:00 Greenwich Mean Time (Etc/Greenwich)' and a 'Current time:' field showing 'Wed May 25 18:25:06 GMT' with a 'Change' link.

At the bottom of the page are three buttons: 'Cancel', '< Back', and 'Next >'.

13. Click **Next**.
The **Network Settings** page displays.
14. Enter a descriptive name in the **Appliance name** field.
15. Select the **Single interface** option.
 ⓘ | **IMPORTANT:** CMS is restricted to a single interface; it cannot be set up with dual interfaces.
16. Enter the **Internal Interface IP address** and **Subnet mask**.

Welcome

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

Central Management

Completion

Network Settings

Enter a name to identify your appliance as well as the IP address and subnet mask for the internal and external network interfaces. If you are using a single gateway in your DMZ, you should select "Single Interface".

Appliance name: * CMS

Dual interfaces Single interface

Internal Interface

IP address: * 192.168.1.1 This is the interface connected to your private internal network.

Subnet mask: * 255.255.255.0

External Interface

IP address: * This is the interface connected to the Internet.

Subnet mask: *

SONICWALL[®]
SECURE MOBILE ACCESS

Cancel < Back Next >

17. Click **Next**.
The **Routing** page displays.
18. From the **Routing mode** field, select **Default gateway**.
19. In the **Default gateway IP address** field, enter the gateway IP address.

Welcome

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

Central Management

Completion

Routing

Network traffic is first sent to a static route (configured later in AMC) if one exists for the destination. If there is no route, traffic is sent to the gateway you specify here.

If you plan to access AMC from a computer on a different subnet than the appliance (192.168.1.1), you must use a default gateway that will pass traffic to that subnet. Alternatively, you can define a static route later in AMC to the subnet from which the appliance is to be accessed.

Routing mode:
Default gateway

Default gateway IP address: * 192.168.1.1 This gateway is used for all network traffic. It must be on the same subnet as the internal (192.168.1.1/24) interface.

SONICWALL[®]
SECURE MOBILE ACCESS

Cancel < Back Next >

20. Click **Next**.
The **Name Resolution** page displays.
21. Enter your domain in the **Default domain** field.
22. Enter the IP address of the primary DNS server into the **DNS Server** field.

23. Click **Next**.
The **Central Management** page displays.
24. Under **Locale**, enter the **Country** and the **Location**.
25. Enable **Central User Licensing** and **Policy Synchronization**.

26. Click **Next** for the **Completion** screen.

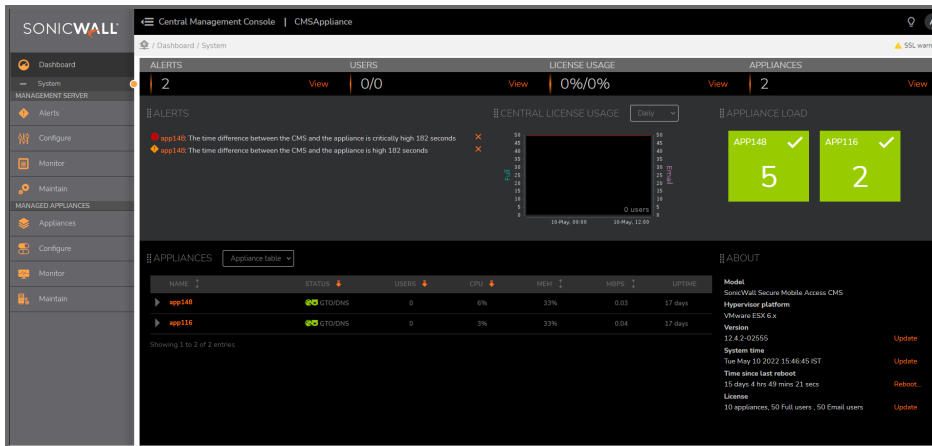


27. Click **Finish**.

The configuration changes are applied and a **Log in** screen displays.



28. Log in with user name as **admin** and the password that you configured.
The **Central Management Console (CMC) Dashboard** page displays.



You can now download and install a CMS license from MySonicWall.com. Refer to [Licensing](#).

Configuring Appliances for Central Management

Topics:

- [Overview](#)
- [Firmware Compatibility with the CMS](#)
- [Enabling Central Management on SMA Appliance](#)
- [Registering an SMA Appliance with the CMS](#)
- [Previously Configured Appliances](#)

Overview

This section describes how to configure SMA appliances for CMS with GTO, so that they become Managed Appliances.

A CMS can manage SMA appliances. Managed Appliances can be any combination of physical and virtual appliances (SMA 6200, SMA 6210, SMA 7200, SMA 7210 and SMA 8200v).

Firmware Compatibility with the CMS

CMS can only manage appliances running firmware that is the same version (or higher) than the CMS. The CMS and all appliances must be running 12.4 firmware (or later) to activate the CMS and Global High Availability (GHA) feature improvements contained in the 12.4 firmware.

CMS can be used to manage appliance that have been upgraded to a new release that is one version above the CMS version. However, newer features on the managed appliances will not work until the CMS is upgraded to the same version as all the managed appliances.

① **IMPORTANT:** It is strongly recommended that the customers/partners upgrade their CMS/SMA appliances to the latest/actively supported feature release and client/platform hotfixes with 12.4 firmware, respectively, and stay up to date from feature set, performance and security standpoint.

For more information about upgrading CMS and its managed appliances, refer to the *SMA 12.4 Upgrade Guide*.

Enabling Central Management on SMA Appliance

Before an appliance can be registered with the CMS, it must first be enabled for Central Management. In addition, the CMS must have an unused appliance license (obtained from the CMS license) before an SMA Appliance can be registered. The administrator must enable Central Management, and copy and paste the auto generated one-time password into the CMS console during registration of the SMA appliance. In addition the administrator must register the appliance with the CMS.

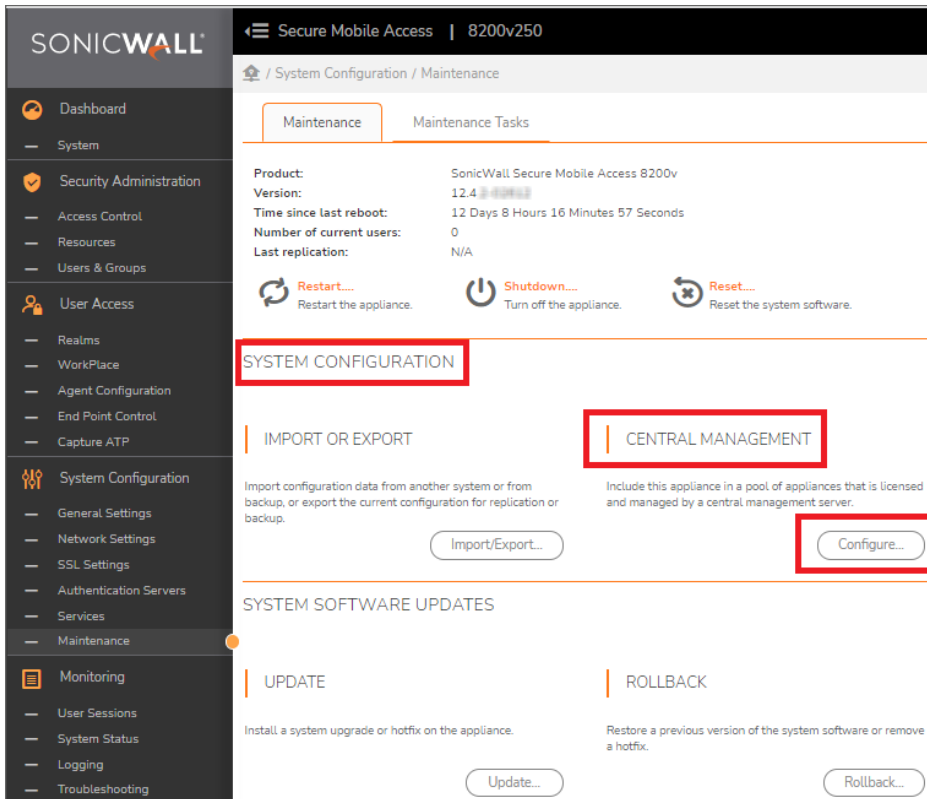
The one-time password is used to establish a secure channel, and all subsequent communications go through the secure channel. The appliance uploads its information (model, version, serial#) to the CMS. The CMS pushes a Leased License to the appliance, and then (if configured), pushes the configuration settings to the appliance.

The managed appliance is now online and ready to accept VPN connections.

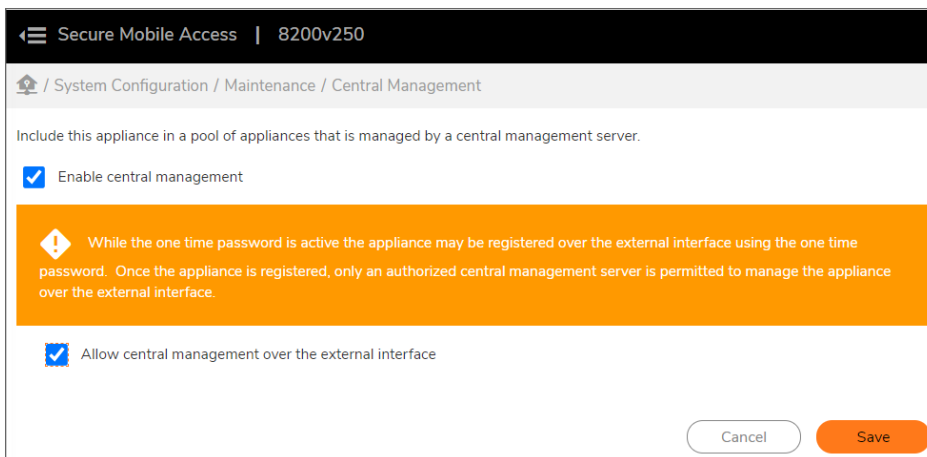
After you have registered a SMA 8200v appliance with a CMS, you can also re-register it to a different CMS by contacting the Sonicwall Support, visit <https://www.sonicwall.com/support/contact-support>.

To enable central management:

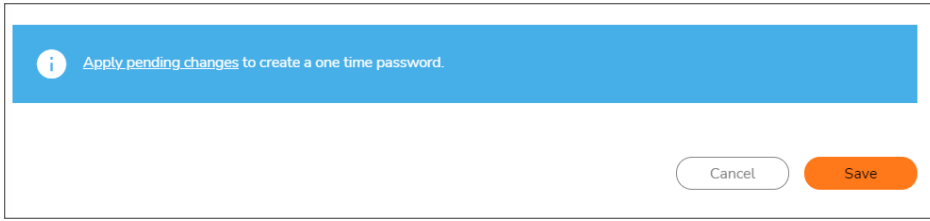
1. On the AMC for the appliance, navigate to **System Configuration > Maintenance**.
2. In the **System Configuration** section, under **Central Management**, click **Configure**.



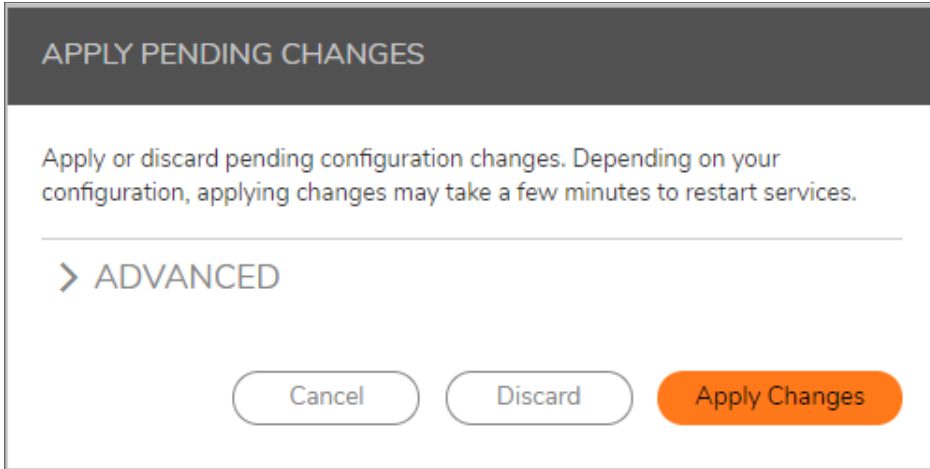
3. Verify that **Enable central management** and **Allow central management over the external interface** are selected.
4. Choose **Save**.



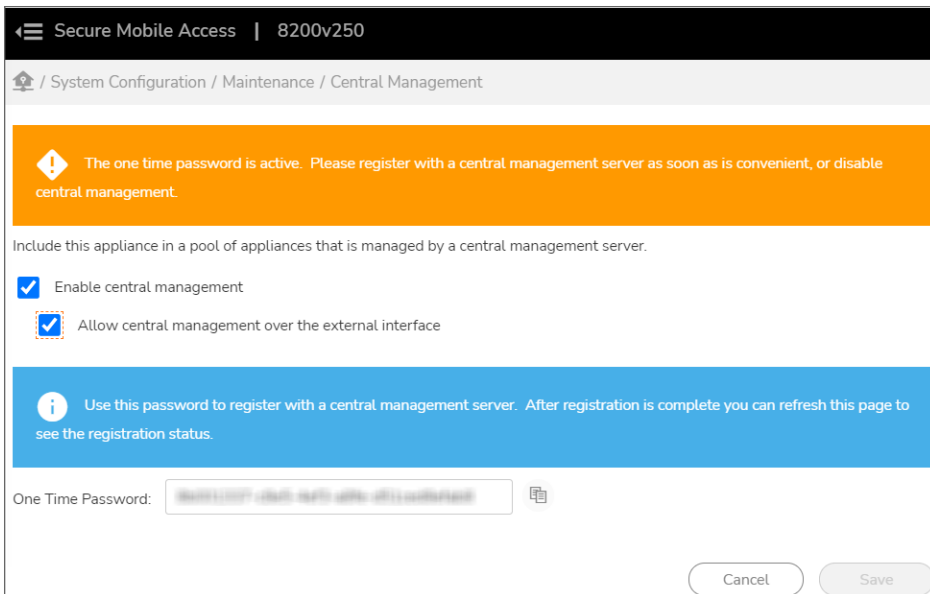
5. Click on the link to **Apply Pending Changes**.



6. Click **Apply Changes**.



The one time password is now active and the appliance is ready to be registered by the CMS.



Registering an SMA Appliance with the CMS

After you enabled the Central management on the SMA Appliance and you must register the SMA appliance with the CMS.

To register the SMA appliance with the CMS, refer to [Add/Remove](#).

Previously Configured Appliances

Standalone appliances that were originally configured from their AMC can be registered with a CMS without affecting the appliance's policy settings.

For information on how to synchronize (or not) policy on an appliance from the CMS, refer to [Synchronize](#).

Using the Management Console Menus

Topics:

- [Overview](#)
- [Dashboard](#)
 - [Alerts](#)
 - [Appliances Pane](#)
 - [Appliance Load](#)
 - [Central License Usage Pane](#)
 - [About Pane](#)
- [Management Server](#)
 - [Alerts](#)
 - [Configure](#)
 - [Monitor](#)
 - [Maintain](#)
- [Managed Appliances](#)
 - [Add/Remove](#)
 - [Configure](#)
 - [Monitor](#)
 - [Maintain](#)

Overview

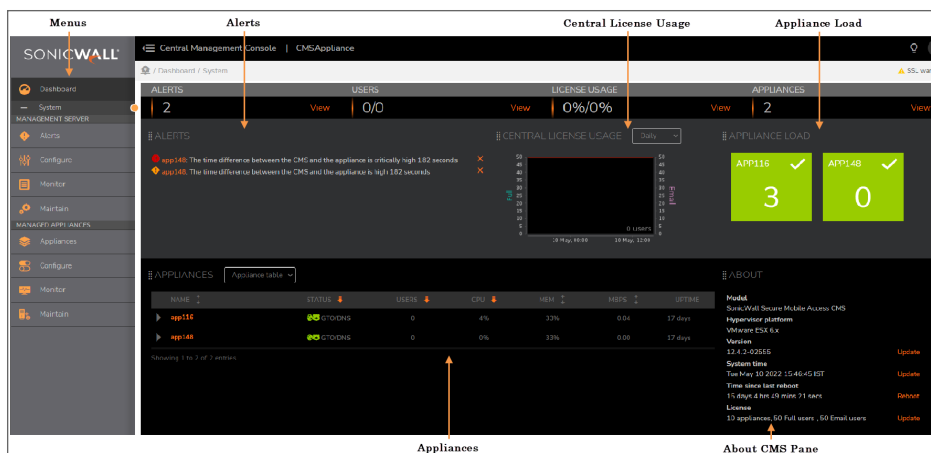
The Central Management Console is the interface you use to manage all the registered VPN appliances. The menu is listed on the left and the content of the window varies depending on the option selected. When you first login to the console, the Dashboard page is the default screen that appears.

The menu has two sections: Management Server and Managed Appliance. Management Server has the commands for central management, licensing and so forth. Managed Appliances have the commands for managing the registered VPN appliances in your infrastructure.

Dashboard

The **Dashboard** page is the first screen that appears after you log in. You can also access it anytime by clicking **Dashboard > System** from the menus.

The Dashboard is divided into the sections illustrated and explained below.



- **Menus** - Contains the commands for central management of your devices.
- **Alerts** - Contains a list of currently active alerts. Select an Alert to view more information.
- **Appliance Load** - An estimate of the current load on an appliance based on metrics such as CPU, Swap Usage, Bandwidth, and memory usage.
- **Appliances** - Shows all online appliances. Select a managed appliance to view information about it. Appliances are sorted starting with the appliance with the most users.
- **Central License Usage** - Displays information about license usage.
- **About** - Displays CMS Information consisting of Model, Hypervisor platform, Version, Hotfixes, System Time, Uptime, and License.

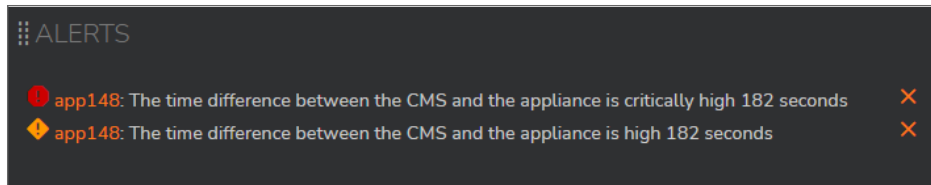
Each pane is independently refreshed with updated information/status.

The Dashboard panes use the following color codes:

- Green (OKAY)
- Yellow (WARNING)
- Red (ERROR)

Alerts

The **Alerts** pane on the Dashboard shows a consolidated view of all currently active alerts that have not been acknowledged by the administrator. These alerts appear when specific thresholds are met. Warnings and Errors are shown on the CMC Dashboard.



Red icons represent critical alerts and yellow icons represent warnings. Errors are listed first, followed by warnings with the most recent being listed at the top of each category.

Alerts can be acknowledged by the administrator by clicking on the X to the right of the it. An acknowledged alert no longer appear in the dashboard, but it re-appears if the state changes. Alerts are automatically removed if the cause of the alert ceases. Click on an individual alert to see the details.

All alerts can be seen when you chose the **Alert** command. Refer to [Alerts](#) for more details.

Appliances Pane

The Appliances pane displays a quick overview of the appliances being managed. It provide real-time data for online, managed appliances and includes:

- Name
- Status
- Users
- CPU usage
- Memory usage
- Mbps, Uptime

The drop down menu on the top, right side provides toggling views of the appliances.

Appliance Table

The Appliance Table is the default view.

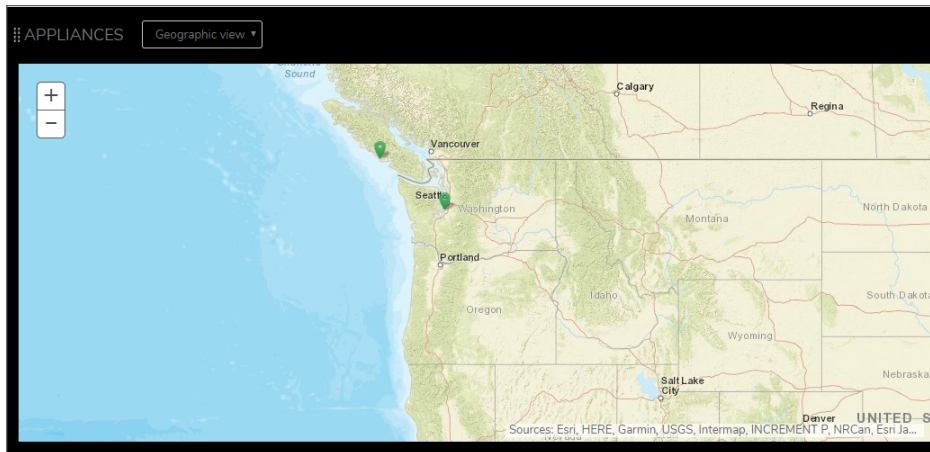
APPLIANCES Appliance table ▾

NAME	STATUS	USERS	CPU	MEM	MBPS	UPTIME
▶ app148	🟢 GTO/DNS	0	7%	33%	0.04	17 days
▶ app116	🟢 GTO/DNS	0	5%	33%	0.04	17 days

Showing 1 to 2 of 2 entries

Geographic View

The Geographic View shows the geographic location of each appliance on a world map.



The Geographic View shows a visual location of the appliance based on its city and country obtained during configuration. You can reposition the icon for an appliance by dragging and dropping the icon to another location. You may need to do this if the icon for an appliance is not correctly positioned on the map, or if multiple appliance icons are positioned too closely to each other.

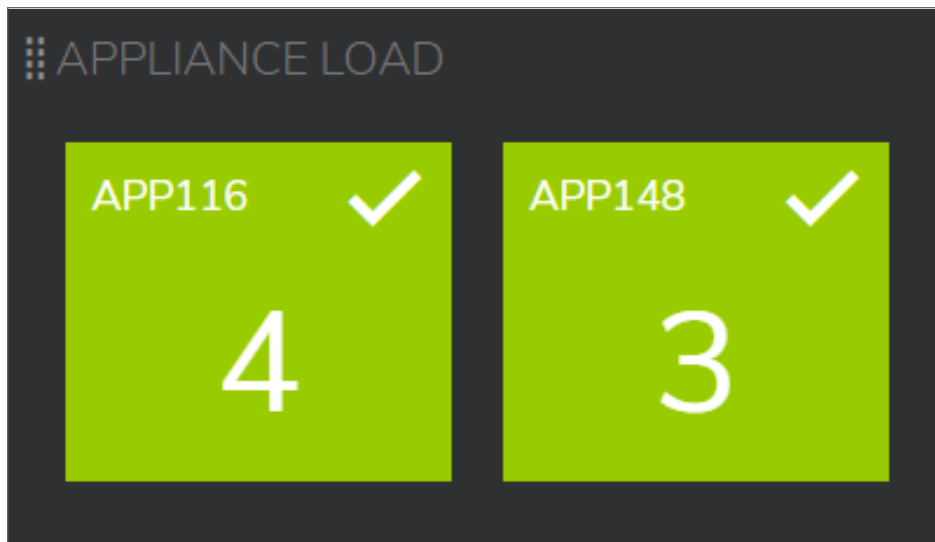
By moving your cursor across the colored icons on the map, details about that appliance appears. In addition, the color of the icon has meaning:

- A blue icon represent the CMS Server and displays Host name and address.
- A green icon represents a selected managed appliance that is online. The interface displays Host, Status, Users, CPU, Memory, Bandwidth information.
- A red icon represents an appliance that is offline.

Zoom (+) and UnZoom (-) buttons allow the map view to be changed. The last map viewed is saved.

Appliance Load

The **Appliance Load** pane displays an estimate of the load level of the appliance based on metrics such as CPU, Swap Usage, Bandwidth, memory usage, and the number of users logged into the appliance. For more information, see the [Appliances Pane](#).



The dial for each appliance displays an estimate of how busy the appliance is:

- Green indicates that the appliance is not very busy.
- Yellow is a warning that the appliance is starting to get busy.
- Red indicates that the appliance is busy or has a 100% load; the user experience may degrade.
- Gray indicates that the appliance cannot be reached.

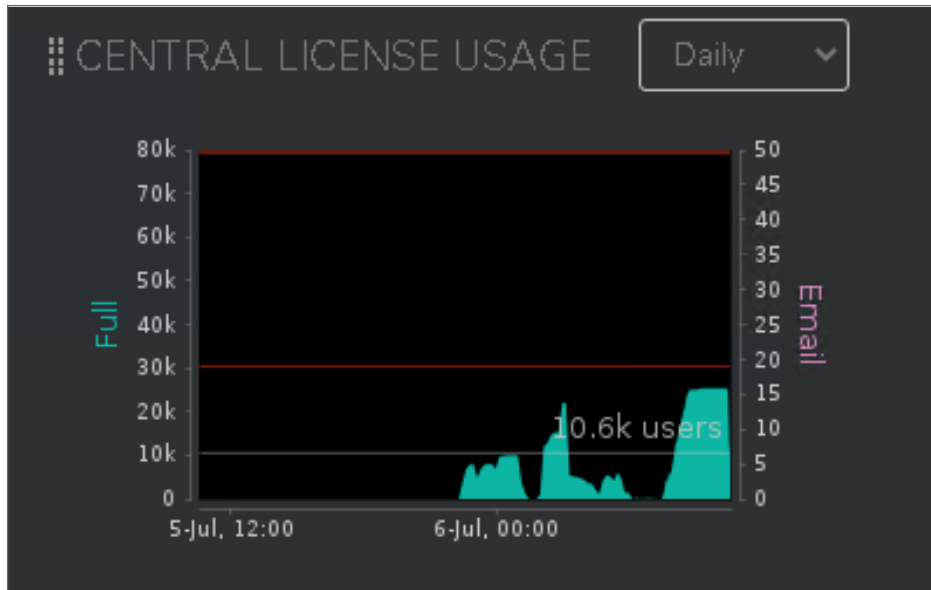
The Appliance load for an appliance is determined by its “load score”.

① **NOTE:** The primary factor in "load score" is distance to the appliance, the closest appliance taking the highest priority. Distance being equal, appliance "load score" is used to determine the appliance that will likely have the best user experience.

- The load score is a combined metric computed from several usage and performance factors (such as CPU, network, and memory) that affect the performance of an appliance, weighted based on their known impact on the remote access experience of connecting users. For example, high CPU usage does not have a major impact on the Load Score for an appliance, but high network bandwidth usage is more highly weighted when the load score for an appliance is calculated.
- When calculating the load score, the differences in the capabilities of the different SMA appliance models in your CMS cluster are taken into account. For example, an SMA 6200 (rated at 2,000 users) with 200 users is expected will show a higher load score than an SMA 7200 (rated at 10,000 users) with 2000 users.
- The impact of different resources is normalized when calculating the load score. For example, users using a significant amount of CPU resources on one appliance will have less impact on the load score than users using excessive bandwidth on another appliance.
- The load score is used by Global High Availability (HA) to determine the preferred appliance toward which user connections and traffic should be routed. For example, if two appliances are located in the same data center or geographic area, Global HA will prioritize the appliance that has the lower load score.

Central License Usage Pane

The **Central License Usage** pane displays the history of CMS user license consumption relative to the maximum license capacity. The drop-down menu allows you to change the display to different time periods, such as Now, Hourly, Daily, Weekly, Monthly, and Quarterly.



The graph displays the number of users as a function of time and colors are used to indicate the status of the licensing:

- Green indicates that the CMS license usage is running within the Central User Licensed capacity.
- Yellow indicates that the license capacity has reached 75%, the default threshold for a CMS license usage warning.
- Red indicates that the license capacity has reached 90% threshold, default threshold for the a CMS license usage alert.

About Pane

The **About** pane displays the information about the Central Management Server:

- Model name
- Hypervisor platform and version number
- Installed hotfixes
- Current system time
- Current uptime statistics
- Licensing summary

ABOUT

Model

SonicWall Secure Mobile Access CMS

Hypervisor platform

Amazon EC2

Version

12.4.2-025316

[Update](#)

System time

Thu Apr 21 22:07:34 GMT

[Update](#)

Time since last reboot

0 days 4 hrs 22 mins 7 secs

[Reboot...](#)

License

10 appliances, 50 Full users , 50 Email users

[Update](#)

Management Server

This section provides information about the Management Server commands:

Topics:

- [Alerts](#)
- [Configure](#)
- [Monitor](#)
- [Maintain](#)

Alerts

CMS generates alerts that are either Warnings or Errors. Alerts are displayed prominently on the CMS dashboard and can also be accessed by selecting the **Alerts** menu option. Alerts typically originate from a condition that occurs on the CMS or on a managed appliance.

This page contains these tabs:

- [View Alerts](#)
- [Configure Alerts](#)
- [Notification](#)

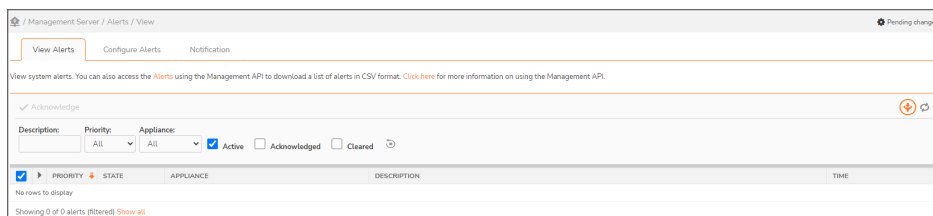
For detailed information about alerts and using alerts with SNMP, refer to [Alerts and SNMP](#).

View Alerts

The **View Alerts** tab is the default view and shows all the alerts in table form. You can sort the table by clicking on the table headings to sort the data.

To view alerts:

1. Navigate to **Management Server > Alerts**.
2. Click the **View Alerts** tab.

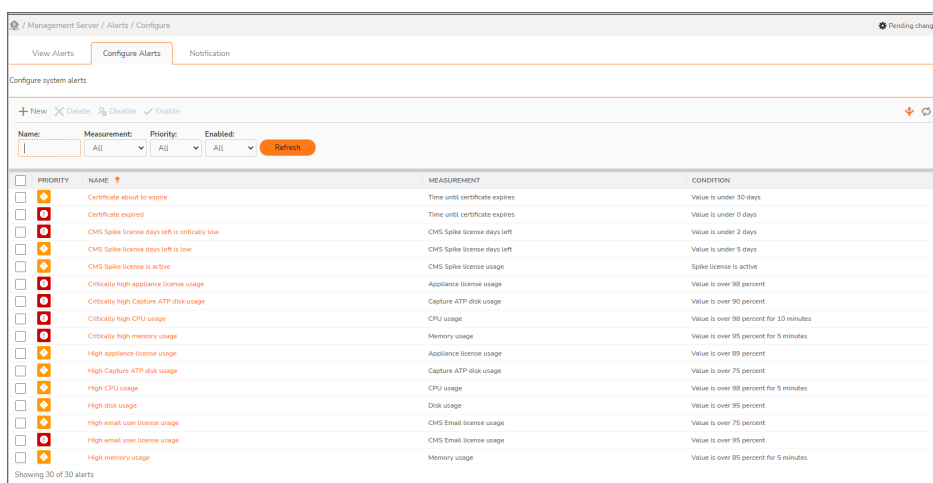


Configure Alerts

Use the **Configure Alerts** tab to add and manage alerts.

To configure alerts:

1. Navigate to **Management Server > Alerts**.
2. Click the **Configure Alerts** tab.



3. Click the **+New** icon.
The **Add Alert Trigger** page displays.
4. In the **Name** field, enter a name for the alert.
5. Select **Alert trigger is enabled** option.
6. Select the **Priority**.
7. Select any other conditions and options that you want.
8. Click **Save**.

The screenshot shows the 'Add Alert Trigger' configuration page. The breadcrumb navigation at the top reads: / Management Server / Alerts / Add Alert Trigger. The form contains the following fields and options:

- Name:** A text input field with a dashed orange border.
- Alert trigger is enabled:** A checked checkbox.
- Priority:** Radio buttons for 'Critical' (selected) and 'Warning'.
- When this measurement:** A dropdown menu showing 'CMS full license usage'.
- Meets this condition:** A dropdown menu showing 'Value is over the threshold'.
- Threshold:** A text input field with '0' and the label 'percent'.
- Activate alert:** Radio buttons for 'As soon as condition is met' (selected) and 'If condition is met for' followed by a text input field with '0' and the label 'minutes'.

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Notification

Use the **Notification** tab to set notifications for alerts.

To set notifications for alerts:

1. Navigate to **Management Server > Alerts**.
2. Click the **Notifications** tab.
3. Select the alerts for which you want to be notified:
 - Critical alerts
 - Warning alerts
 - Acknowledged alerts
 - Cleared alerts
4. Under **Email Settings**, enter the Email address from which alert notifications is sent.

- To add an Email address to send alert notifications to, click the (+) New icon.
- Enter the **Name** and **Email Address** of the recipient to be notified and click **OK**. Repeat to add more recipients.

Management Server / Alerts / Notification

View Alerts Configure Alerts **Notification**

Configure settings for alert notification

Notify recipients of:

- Critical alerts Critical alerts will generate **SNMP traps** if SNMP is enabled with trap receivers.
- Warning alerts
- Acknowledged alerts
- Cleared alerts

EMAIL SETTINGS

Email messages will be sent for the above events.

! Email alerts will not be sent because SMTP is not enabled. Go to the [SMTP settings](#) page to configure SMTP.

From address: Alert notifications use the [SMTP settings](#) to send email messages.

Send email to the following recipients:

+ New X Delete

<input type="checkbox"/>	NAME	ADDRESS	ENABLED
No rows to display			

Cancel Save

- Click **Save**.

Configure

The **Configure** option allows you to set various options for the Central Management Console. Navigate to **Management Server > Configure** to see the options.

Topics:

- [Central Management Settings](#)
- [CMS Address Pool](#)
- [Licensing](#)
- [General Settings](#)
- [Administrators](#)
- [Network Settings](#)
- [SSL Settings](#)
- [Services](#)

Central Management Settings

Use the Central Management Settings option to configure CMS location, Central User Licensing, Global Traffic Optimizer, and Policy Synchronization.

To configure the Central Management Settings:

1. Navigate to **Management Server > Configure**.
2. Click on **Central Management**.
The **Central Management** page displays.
3. Under **Locale**, select your **Country or region** and enter your **Location**.
4. Under **Central User Licensing**, select **Enable central user licensing**. The current CMS license will support **50 users and 50 email users across all appliances**.
5. Under **Global Traffic Optimizer Service**, select **Users connect to this global high availability service from anywhere in the world and are routed to a nearby appliance**.

NOTE: Central User Licensing must be enabled to activate the Global Traffic Optimizer service.

The screenshot shows the 'Central Management' configuration page. At the top, there is a breadcrumb trail: 'Management Server / Configure / Central Management'. Below this, a descriptive text states: 'This central management server manages the licensing and configuration for a collection of appliances.' The page is divided into three main sections: 'LOCALE', 'CENTRAL USER LICENSING', and 'GLOBAL TRAFFIC OPTIMIZER SERVICE'. In the 'LOCALE' section, there is a 'Country or region' dropdown menu currently set to 'N/A' and a 'Location' text input field with the example 'Seattle, WA'. The 'CENTRAL USER LICENSING' section has a checked checkbox for 'Enable central user licensing. The current CMS license will support 50 users and 50 email users across all appliances'. The 'GLOBAL TRAFFIC OPTIMIZER SERVICE' section has a checked checkbox for 'Users connect to a global high availability service from anywhere in the world and are routed to an available appliance.' Below this, there are two blue informational boxes: 'Each service domain name must be delegated in public DNS' and 'Custom GTO services can be created using central policy resources'. At the bottom, there are '+ New' and 'X Delete' buttons, and a table with columns for 'NAME', 'DESCRIPTION', 'DOMAIN', and 'APPLIANCES'. The table currently shows 'No rows to display'.

6. Under **Policy Synchronization**, select **Enable pushing policy configuration from this server to managed appliances**. This feature is recommended so that users will have a consistent experience on all GTO-enabled appliances and the required **Address Pools** option.
7. Under **Address Pools**, select one of the following:

- All appliance address pool settings configuration is controlled by the central policy on the CMS (recommended).
- Each appliance has its own address pool configuration (not recommended).
For configuring CMS address pool and to use convert address pool option, refer to [CMS Address Pool](#).

8. Under **Authentication Servers**, select one of the following:

- Appliance share the same authentication servers.
- Each appliance has its own authentication server and OTP settings.

Management Server / Configure / Central Management

POLICY SYNCHRONIZATION

Enable pushing policy configuration from this server to managed appliances.
By default, configuration data on the managed appliances will be overwritten. To preserve certain settings on the appliances, specify exclusions here.

ADDRESS POOLS

All appliance address pool configuration is controlled by the central policy on the CMS (recommended)
Overwrites the address pool settings on the managed appliances. Use CMS Address Pools to specify per-appliance address pools.

Each appliance has its own address pool configuration (not recommended)
Retains address pool settings on the managed appliances. This requires address pool names to be in sync between the CMS and Managed Appliances.

[Convert address pools...](#) Use this option to convert the CMS configuration to use central configuration for all appliance-specific address pools by converting the named address pools to CMS Address Pools. You can preview the changes before completing the conversion.

AUTHENTICATION SERVERS

Appliances share the same authentication servers
Overwrites the authentication server and OTP settings on the managed appliances. OTP settings include SMS, SMTP and TOTP services.

Each appliance has its own authentication server and OTP settings.
Retains authentication settings on the managed appliances, except in the case of a PKI server: trusted CA certificates cannot be retained.

9. Under **Other Service**, select the following services:

Once the configurations are saved and pushed, a warning message is displayed indicating that the settings are pushed to CMC or overwritten on synchronization with AMC.

NOTE:

1. Enable the syncing of settings for the services by selecting the checkbox.
2. For fresh installation, the four service options (SSH, Syslog, NTP, and Ping (ICMP)) are enabled. For upgrade or import, these options are disabled.

Service Option	Description
Secure Shell (SSH)	Includes SSH service enabled/disabled, allowed remote hosts, and authorized keys.

Service Option	Description
Syslog	Includes the syslog servers to which all log information is sent.
NTP	Includes NTP service enabled/disabled and NTP servers.
Ping (ICMP)	Includes ping (ICMP) enabled/disabled and supported network interfaces (internal, external, or both).

10. Under Advanced, in the **Pool IP** field, enter the CMS IP address that is reachable by managed appliances. **ⓘ | NOTE:** This is required only if the CMS internal address is not reachable by managed appliances.

OTHER SERVICES

Appliances share the same configuration for the following services.

<input type="checkbox"/> Secure Shell (SSH)	Includes SSH service enabled/disabled, allowed remote hosts, and authorized keys.
<input type="checkbox"/> Syslog	Includes the syslog servers to which all log information is sent.
<input type="checkbox"/> NTP	Includes NTP service enabled/disabled and NTP servers.
<input type="checkbox"/> Ping (ICMP)	Includes ping (ICMP) enabled/disabled and supported network interfaces (internal, external, or both).

ADVANCED

Pool IP:

The CMS IP address that is reachable by managed appliances. This is required only if the CMS **internal address** is not reachable by managed appliances.

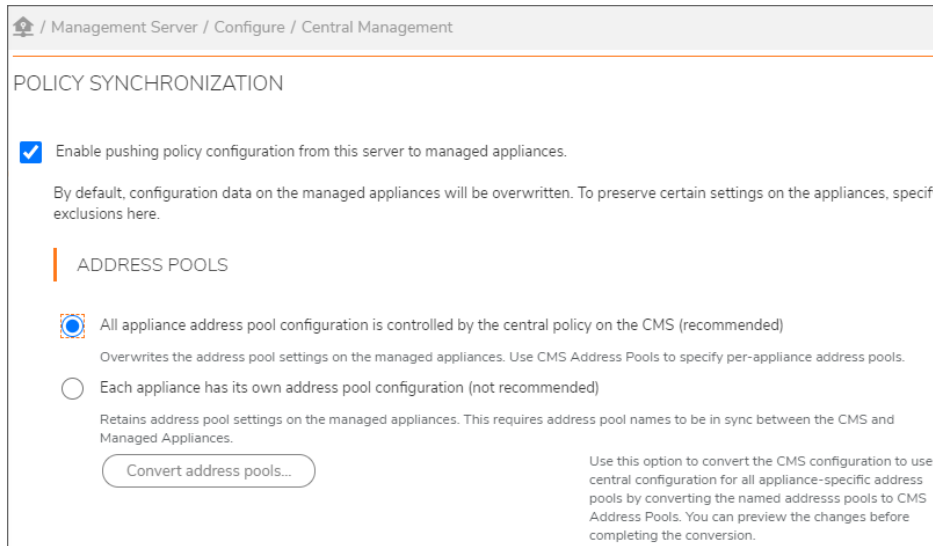
11. Click **Save**.

CMS Address Pool

The following enhancements are in CMS Address Pool and each managed appliance can now:

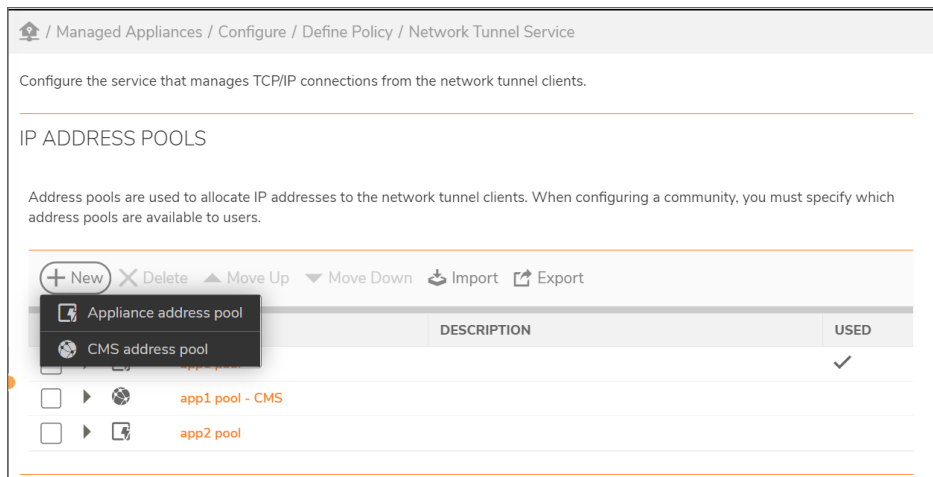
- Have a unique address pool.
- Share an address pool configuration with one or more other appliances.

- Use a default address pool.



Follow the instruction to configure the CMS address pool.

1. Navigate to **Managed Appliance > Configure > Define Policy**
2. Under **User Access** group, click **Network Tunnel Service**.
The Network Tunnel Service page displays.
3. In the **IP Address Pools**, click **+New** and select **Appliance address pool**.



4. Enter Name, description, and select the address pool to create the appliance-specific pool.
5. Click **Save**.
6. Navigate to **Management Server > Configure > Central Management**.
7. Under **Policy Synchronization**, you have the following options.

- To convert CMS address pool (If CMS deployed and you have using appliance-specific address pools)
 - a. Click **Convert address pools..**, this option convert the CMS configuration to use central configuration for all appliance-specific address pools by converting the named address pools to CMS address pools.
 - b. Click **Convert** to convert the Address pools to new CMS address pools successfully.

OR

- To create CMS address pool.
 - a. In the **IP Address Pools**, click **+New** and select **CMS address pool** to create CMS address pool.
8. Enter Name, description, and choose the default address pool to create a CMS address pool to configure appliance-specific address pools for managed appliances.
 9. Click **Save**.
 10. After CMS address pool is created, click the CMS address pool in the **IP Address Pools** page.
 11. Under the **Appliance Address pools**, for each appliance, choose the Appliance Address Pool drop-down and select **Use default** or create appliance-specific address pool.
 12. Click **Save**.

Licensing

Use the **Licensing** option to review and manage the software licenses for CMS.

To manage the licenses:

1. Navigate to **Management Server > Configure > General setting**.
2. Under **Licensing**, click **Edit**.
The **Manage Licenses** page displays.
3. Review your license information.
4. Under **Online licensing**:
 - Click **Register**. Log in to your MySonicWall account to review and manage with your licensed services on MySonicWall.

Management Server / Configure / General Settings / Manage Licenses

Review and manage the software licenses for the CMS.

MySonicWall License Manager

mySonicWall.com Login

mySonicWall.com is a one-stop resource for registering all your SonicWall Internet Security Appliances and managing all your SonicWall security service upgrades and changes. mySonicWall provides you with an easy to use interface to manage services and upgrades for multiple SonicWall appliances. For more information on mySonicWall, please visit the [FAQ](#). If you do not have a mySonicWall account, please click [here](#) to create one.

Please enter your existing mySonicWall.com username (or email address) and password below:

MySonicWall username(email):

Password:

[Forgot your Username or Password?](#)

- Expand the **Advanced** section to activate spike license. Select **Automatically Activate spike license**.

Management Server / Configure / General Settings / Manage Licenses

Review and manage the software licenses for the CMS.

Product: SonicWall Secure Mobile Access CMS
 License holder: SonicWall Engineering
 Maximum concurrent users: Full: 0 Email: 0
 Maximum appliances: 10
 Appliance serial number: N/A
 Authentication code: N/A
 Licensing mode: Manual

COMPONENT	LICENSE TYPE
Managed appliances: 10	View Details
Central email licenses: 50	View Details
Capture Advanced Threat Protection	View Details
FIPS	View Details
Central user licenses: 50	View Details

ONLINE LICENSING

This appliance is not registered with MySonicWall. Choose **Register** to register this appliance with your MySonicWall account.

ADVANCED

The CMS will automatically activate a spike license during periods of high usage if it is available. Use this setting to override this behavior.

Automatically activate spike license

⚠ Disabling automatic spike activation is not recommended. The system will not be able to increase the license capacity when user demand increase to ensure uninterrupted access.

MANUAL LICENSING

If this system does not have access to the internet, you can upload a license file. Log in to your MySonicWall account to obtain the license file.

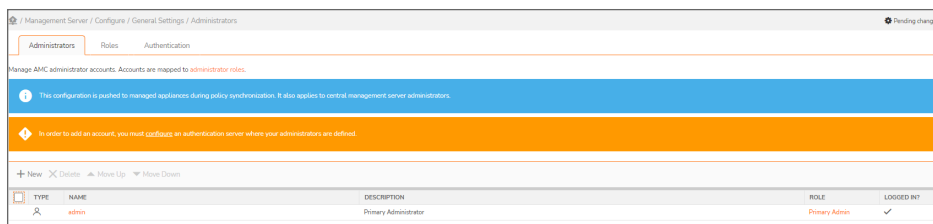
- Under **Manual Licensing**, import the license file. Log in to your MySonicWall account to obtain the license file.

Administrators

Use the **Administrators** option to define who the administrators are and what authentication server are used for managing the Central Management Server.

To configure the Administration settings:

1. Navigate to **Management Server > Configure > General Settings**.
2. Under **Administrators**, click on **Edit**.
3. Select any of the three tabs: **Administrators**, **Roles**, and **Authentication**.
4. Click **+New** to add an account and to manage AMC administrator accounts.
5. When your administrators are defined, click **Save**.



General Settings

Use the **General Settings** to control security settings for users and set the date and time.

To configure the General Options:

1. Navigate to **Management Server > Configure > General Settings**.
2. Under **Appliance Options**, click on **Edit**.
The **Appliance Options** page displays.
3. Set the credential lifetime in minutes. This refers to the length of a user session. If it exceeds the time specified the user is asked to re-authenticate.
4. Set the date and time, if needed.

5. Click **Save**.

Management Server / Configure / General Settings / Appliance Options

CLIENT SECURITY SETTINGS

Control security settings for users. You can also enhance security using [End Point Control \(EPC\)](#).

Credential lifetime: * minutes If the length of a session exceeds the time specified, the user is prompted to reauthenticate.

DATE/TIME

To set the management server time click **Change** next to the current time, or [click here](#) to configure the management server to synchronize with one or more NTP servers. To set the time zone referenced on the management server and in the system logs, click **Change** next to the time zone.

! Apply or discard pending changes before modifying the date, time, or time zone.

Current system time: Thu Apr 21 2022 22:36:39 GMT
Time zone: GMT+00:00 Greenwich Mean Time (Etc/Greenwich)

Cancel Save

Network Settings

Use **Network Settings** to modify server IP address, routing and name resolution.

- ① **NOTE:** It is not recommended to modify the network interface settings for AWS, Azure and KVM instances. Modifying the network interface settings will cause CMS to crash.

To configure the network settings:

1. Navigate to **Management Server > Configure > Network Settings**.
2. The **Network Settings** page appears
3. Click **Edit** to configure any of the **Basic**, **Routing**, or **Name resolution** settings.

4. When settings are finished, click **Save**.

Management Server / Configure / Network Settings

BASIC

Single interface, single node Edit

CMS name:	SMAAppliance
CMS public domain:	ap-south-1.compute.internal
Private address:	172.31.0.10
ICMP pings:	Disabled

ROUTING

Routing mode:	Default gateway	Edit
Default gateway:	172.31.0.1	
Static routes:	0 routes defined	

NAME RESOLUTION

Private search domains:	N/A	Edit
DNS servers:	172.31.0.1	
WINS server:	N/A	
Windows domain:	N/A	

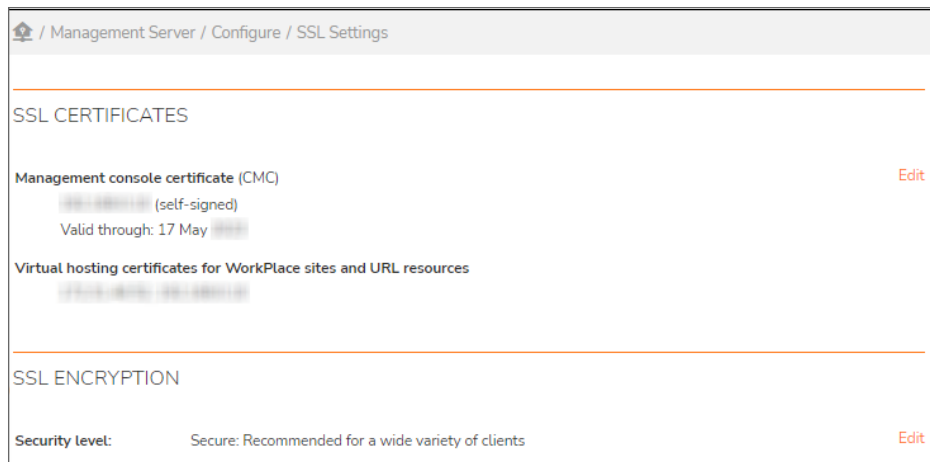
SSL Settings

Use the **SSL Settings** option to modify the management console certificate and SSL settings.

To configure SSL settings:

1. Navigate to **Management Server > Configure > SSL Settings**.
The **SSL Settings** page displays.
2. Click **Edit** for the item you want to edit: **SSL certificates** or **SSL encryption**.
3. Make the desired changes.
4. When the changes are finished, click **Save** and **Pending Changes**.

5. Click **Apply Changes**.

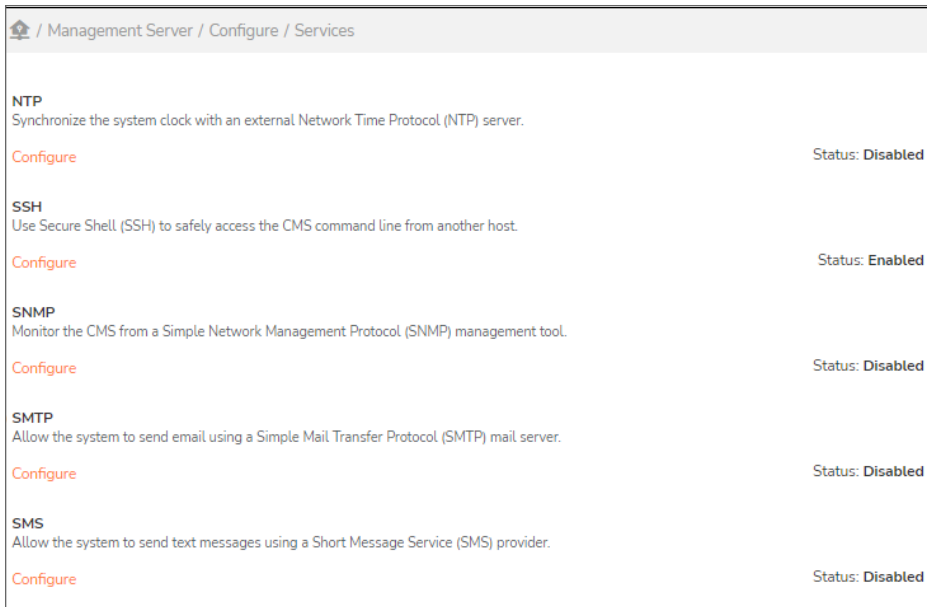


Services

Use the **Services** option to modify the settings for server services like NTP, SSH, SNMP and SMTP.

To configure Network Services:

1. Navigate to **Management Server > Configure > Services**.
The **Services** page appears.
2. Click **Configure** for which you want to configure: **NTP**, **SSH**, **SNMP**, **SMTP**, or **SMS**.
For more information to configure the Service, refer to *SMA 12.4 Administration Guide*.
3. Make the desired changes.



4. When the changes are finished, click **Save**.

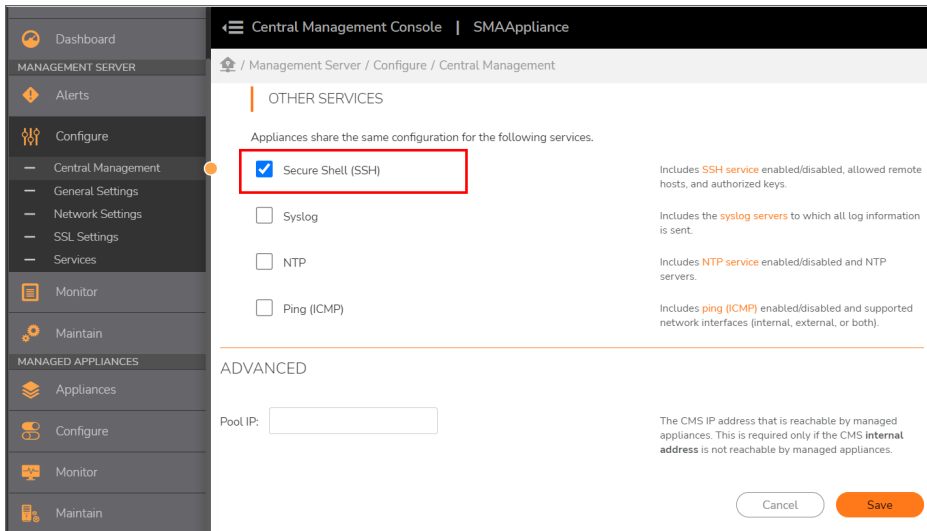
Manage SSH settings from CMS

For CMS Administrator, it is difficult to manage authorized keys when configuring on multiple appliances. To overcome this scenario, SMA is enhanced to manage the SSH settings centrally from CMS. You can configure SSH once in CMS and use the same keys to access SSH in all the managed appliances and CMS after successful completion of Policy Synchronization.

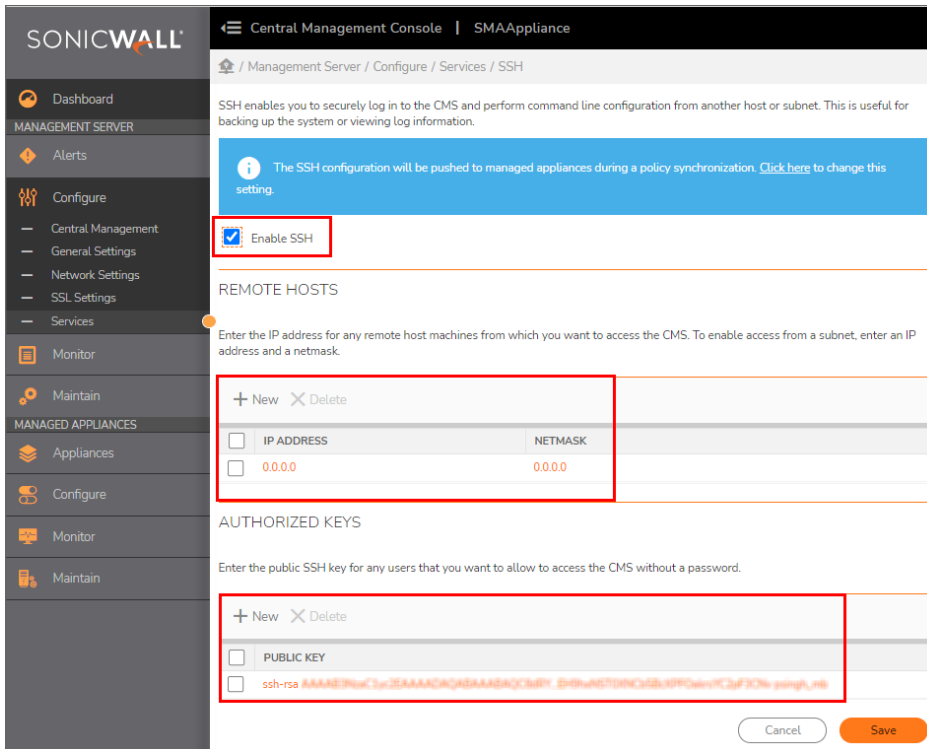
To manage SSH settings from CMS:

1. Log in to CMS.
2. Navigate to **Management Server > Configure > Central Management**.
3. Under **Other Services**, select **Secure Shell (SSH)**.

① **NOTE:** It enables the syncing of the SSH settings. **Policy synchronization** option should be enabled.



4. Click **Save**.
5. Navigate to **Management Server > Configure > Services** page.
6. Under SSH, click **Configure**
7. In the SSH page, select **Enable SSH** and configure SSH settings with remote hosts and public key.



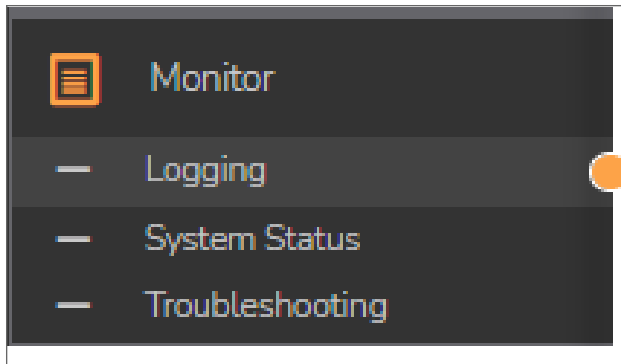
8. Click **Save**.

① | **NOTE:** The latest settings are activated on the appliance only after the completion of synchronization.

9. Synchronize all the managed devices.
10. Access the SSH of managed appliance or CMS in remote hosts using the public key if specified in the CMS.

Monitor

The **Monitor** option allows you to set various options for monitoring. Navigate to **Managed Server > Monitor** to see the options.



- Click **Logging**.
Select **View Logs** tab, to view the system logs and configure the log settings.
Select **Configure Logging** tab, to configure the logging settings. Make the changes and click **Save**.
Select **Managed Appliances** tab, to configure and manage the logging settings for all the managed appliances. Make the changes and click **OK**. For configuring the logging setting for Managed appliances, refer to [Configure the logging setting for Managed appliances](#).
- To view health metrics and system information for the CMS, click **System Status**.
- To ping, lookup, routes, network traffic, snapshot, client, and Hosts, click **Troubleshooting** and select the respective tabs to configure.

Configure the logging setting for Managed appliances

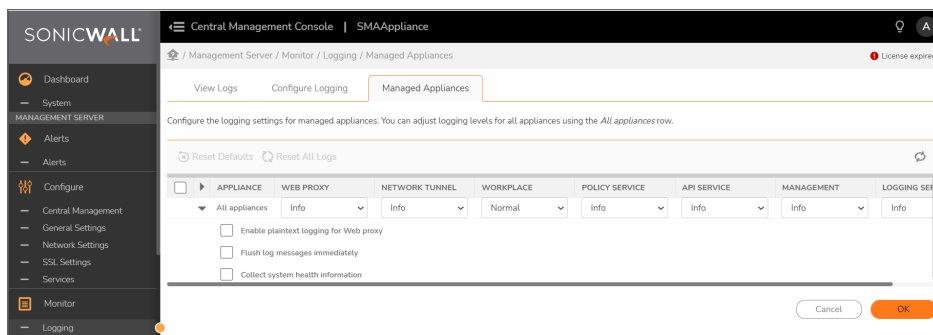
The following are settings you can modify:

- 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:

1. In CMS, **Management Server > Configure > Central Management**, under **Authentication Servers** section, ensure **Appliances share the same authentication servers** is selected.

2. Navigate to **Management Server > Monitoring > Logging**.
3. Select the **Managed Appliance** tab.
4. Click on **All appliances** to adjust logging levels for all appliances or click on specific appliance.
 - Select **Enable plain text logging for Web proxy**
 - or
 - Flush log messages immediately**
 - or
 - Collect system health information**.



5. Click **OK**.

Maintain

The **Maintain** option allows you to set various options for monitoring. Select **Managed Server > Maintain > Maintain Server** to see the options.

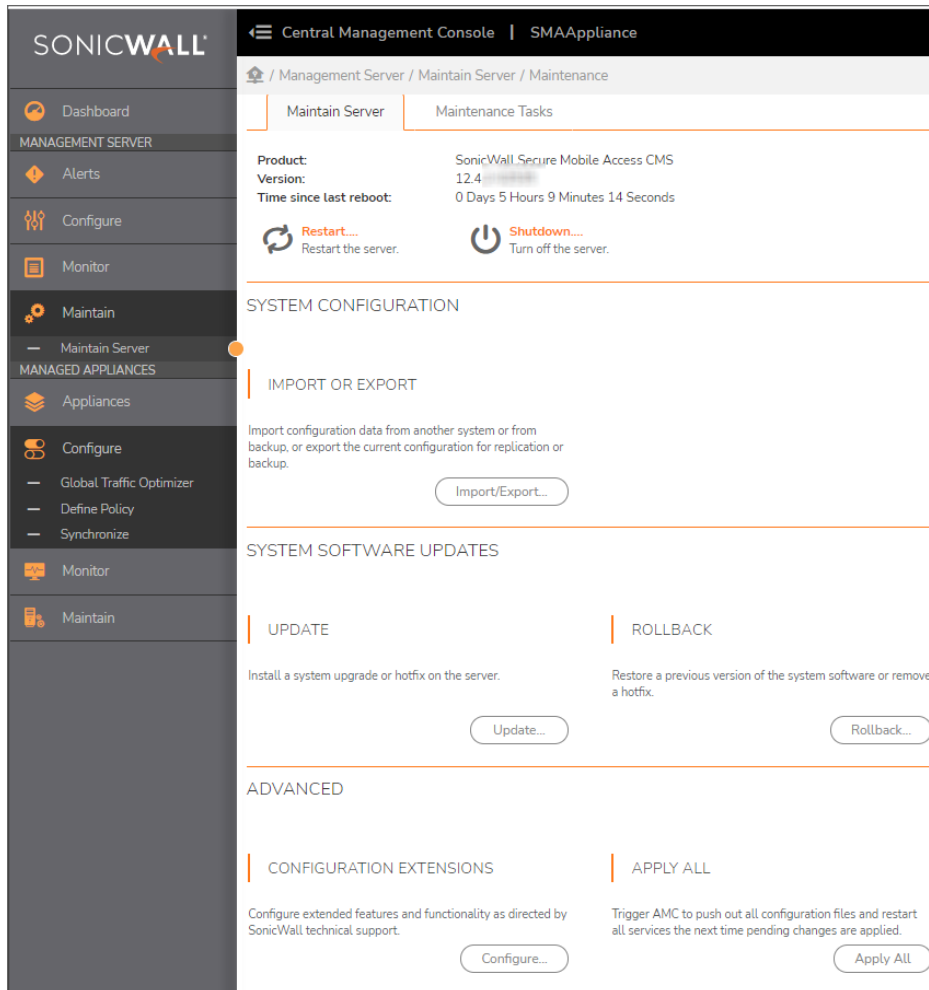
Maintain Server

To maintain the CMS:

For more information on the settings options in Maintain Server, refer to *SMA 12.4 Administration Guide*.

1. Select **Management Server > Maintain > Maintain Server**.
The **Maintain Server** page appears.
2. Do any of the following:
 - To restart the CMS, click **Restart**.
 - To shutdown the CMS, click **Shutdown**.
3. To import or export a system configuration file, click **Import/Export**. Provide additional information on the next window.
4. To update the system software to a newer version, click the **Update** button.
5. To rollback the system software to a previous version, click the **Rollback** button.
6. To configure the extensions and the Global overrides, under **Advanced**, click the **Configure** button.

7. To trigger AMC to push out all configuration files and restart all service the next time pending changes are applied, click the **Apply All** button.

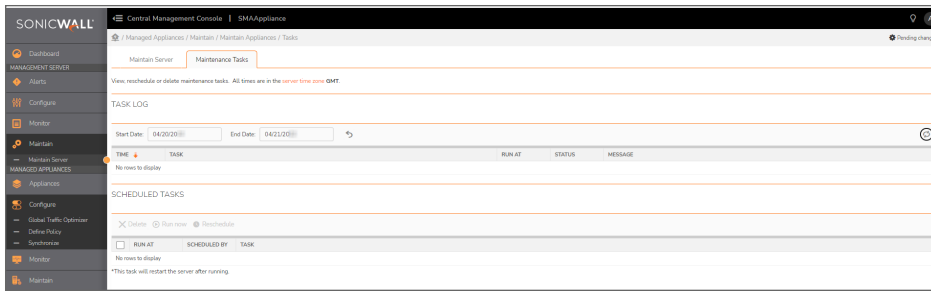


Maintenance Tasks

To view the maintenance tasks:

1. Select **Management Server > Maintain Server > Maintenance**.
2. Click the **Maintenance Tasks** tab. On the **Task Log** page, you can view the tasks that are scheduled.
3. Filter the **Task log** table by setting a **Start Date** and **End Date** and clicking the **Refresh** icon.

- In the **Scheduled Tasks** panel, you can select a task and **Delete**, **Run now**, or **Reschedule**.



Managed Appliances

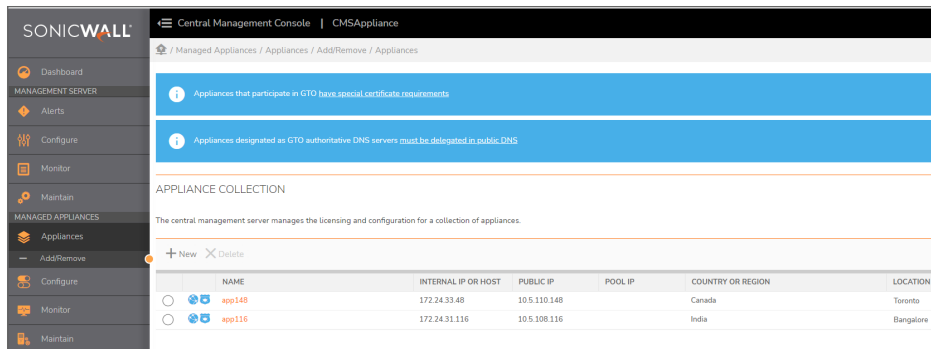
This section provides information about the Managed Appliances commands:

Topics:

- [Add/Remove](#)
- [Configure](#)
- [Monitor](#)
- [Maintain](#)

Add/Remove

The Add/Remove option allows you to manage the licensing and configuration for collection of appliances from a central location. Navigate to **Managed Appliances > Appliances > Add/Remove** to see the **Appliance Collection**.



To add/register a new appliance:

- NOTE:** Same procedure steps to register an SMA appliance with the CMS and adds it to the CMS list.

1. Under the **Appliance Collection** section, click the **(+) New** icon.
2. In the **Name** field, enter a name for the new appliance. For example, **Seattle-01**.
3. In the **Management address** field, enter the IP address for the new appliance.
4. In the **One Time Password** field, enter the one time password obtained from the **Maintenance > Central Management** page of the SMA appliance.
5. Click **OK**.

This registers the appliance with the CMS and adds it to the CMS list. The dialog changes with more options.

NOTE: The client certificate warning, DNS name field, and Public IP field are only visible when CMS is enabled for GTO.

6. In the **Display Name** field, enter the name you want displayed for this appliance.
7. In the **Host name** field, enter a unique DNS-legal name for this appliance, for example **seattle01**.
8. In the **Management address** field, enter the IP address for the appliance.
9. In the **Public IP** field, enter the internet-visible, public IP address for this appliance.

NOTE: The **Public IP** should be the address by which remote users will access this appliance. The default IP address is the external IP address of the appliance. The public IP address may be different from its external IP address if the public WAN addresses are using NAT at the DMZ.
10. If the appliance has an IPv6 address, enter that IP address in the **Public IPv6** field.
11. In the **Pool IP** field, enter the IP address that is reachable by other appliances by the same CMS. This IP address is only required if the **Public IP** of this appliance cannot be reached by the other managed appliances.
12. From the **Country** menu, select the country where the appliance is located.
13. In the **Location** field, enter the city, state, or province where the appliance is located.
14. Click **Save**.

EDIT APPLIANCE SETTINGS

Display name:*	<input type="text" value="ma1"/>	The display name for this appliance
Host name:*	<input type="text" value="ma1"/>	The host name for this appliance
Management address:*	<input type="text" value="192.168.1.100"/>	An appliance IP address or host name that is reachable from the CMS
Public IP:*	<input style="border: 2px solid orange;" type="text" value="192.168.1.100"/>	The appliance IP address that is routable from the Internet, typically this is the appliance external IP address
Public IPv6:	<input type="text"/>	The appliance IPv6 address that is routable from the Internet, typically this is the appliance external IPv6 address
Pool IP:	<input type="text"/>	The appliance IP address that is reachable by other managed appliances. This is only required if the appliance Public IP is not reachable by other managed appliances.
Country or region:	<input type="text" value="United States"/>	The country or region where this appliance is located
Location:	<input type="text" value="Milpitas, CA"/>	The city, state or province where this appliance is located
<input checked="" type="checkbox"/> Enable Global Traffic Optimizer Service		Participate in global high availability services
	<input type="text" value="ma1.cms.sea.eng.sonicwall.com"/>	The DNS name for this appliance
i This appliance is a public DNS delegation target and must be manually delegated in public DNS		
<input checked="" type="checkbox"/> DNS authoritative server		This appliance will serve as a DNS authoritative server for all GTO services
<input type="checkbox"/> Disable this appliance		Users connecting to GTO services will not be routed to this appliance. Existing users on this appliance will not be affected. A disabled appliance can serve as a DNS authoritative server.
User capacity:	<input type="text" value="100"/>	For appliances in the same location, user sessions will increase relative to their user capacity. As the user count approaches capacity, the load score will be affected.
	The recommended maximum capacity is 5000 users	

To stop managing an appliance:

1. Select the appliance you want to delete.
2. Click the **X Delete** icon.
3. Click **OK**.
4. Click **Pending Changes** to apply pending changes on the appliance.
5. Under Advanced, click **Apply Changes**.

Configure

Topics:

- [Overview](#)
- [Configuring the Managed Appliances](#)
- [Support multiple policies with CMS and shared licensing](#)

Overview

An administrator can import policies from an existing appliance and define configurations. Policies can be applied to all appliances or just a subset. An existing managed appliance configuration may be partially imported into the CMS to startup the CMS global configuration.

The first time the CMS synchronizes a policy with an appliance, it overwrites the policy on the appliance. This is equivalent to the appliance partially importing the CMS configuration. After the initial policy synchronization, further policy synchronizations replicate the CMS configuration onto the appliance.

The policy settings that are replicated during synchronization are:

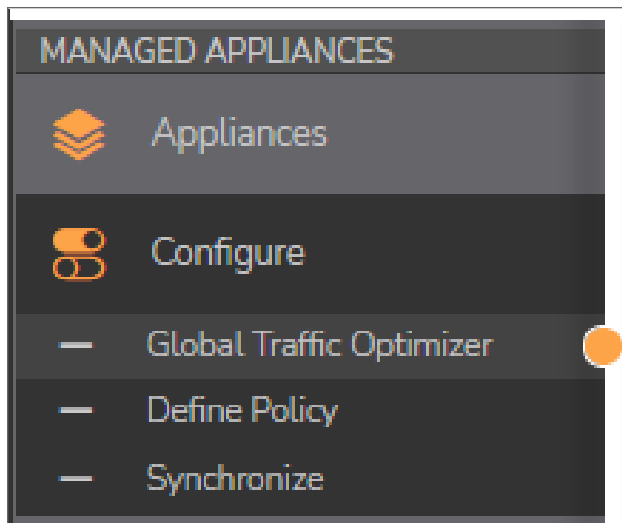
- Security policy, including access control rules and EPC configuration
- Network resources
- Users and groups
- Realms
- Authentication servers
- WorkPlace shortcuts
- CA certificates
- Certificate revocation lists downloaded from a remote CDP (CRL distribution point)
- Agent configuration, including graphical terminal agents (Citrix and Windows Terminal Server) and Web browser profiles
- Local user accounts
- Single sign-on profiles
- NTP, SSH, SMTP, and SMS (optionally replicated)

The policy settings that are not replicated during synchronization are:

- Network settings, including IP addresses, routing information, name resolution settings (DNS and WINS), and the settings for the network services (SNMP)
- License files
- SSL certificates
- WorkPlace configuration data (customized templates)
- Administrator user accounts and role definitions

Configuring the Managed Appliances

Navigate to **Managed Appliances > Configure** to see the configuration options.

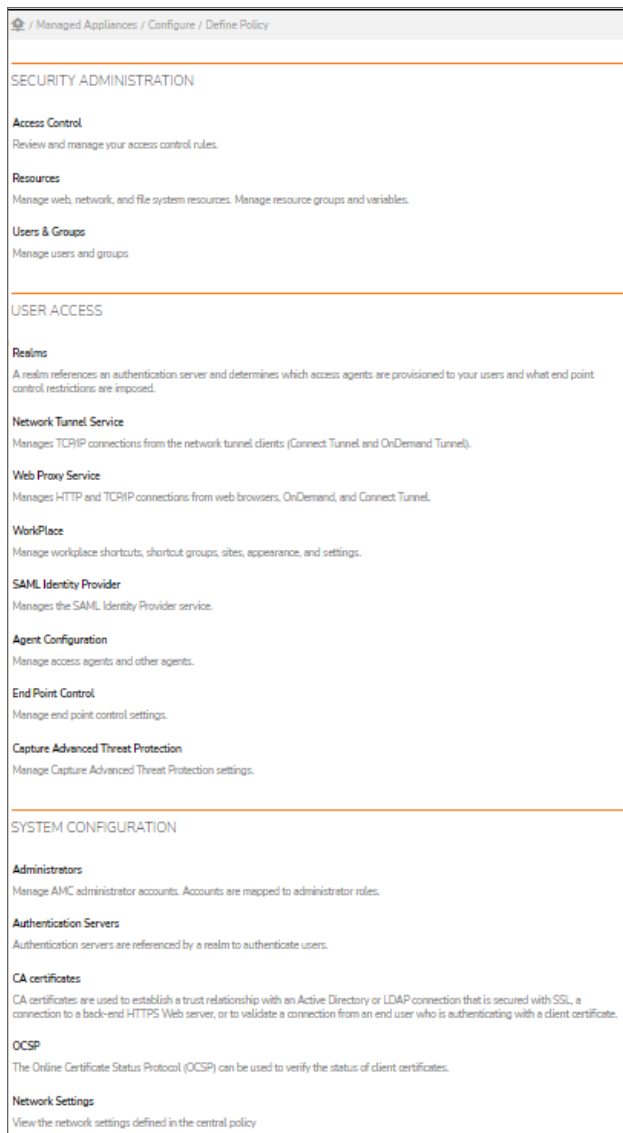


- The **Global Traffic Optimizer** option provides access to configure and manage the Global Traffic Optimizer service. (For more information about Global Traffic Optimizer, see [Introduction to Global HA and GTO](#)).
- The **Define Policy** option provides access to the Security Administration, User Access, and System Configuration policy pages.
- The **Synchronize** option allows you to view and schedule policy synchronization events.

Define Policy

To define policies:

1. Navigate to **Managed Appliances > Configure**.
2. Click **Define Policy**.



3. Under **Security Administration**, **User Access**, and **System Configuration** sections, you can define the policies. For configure support multiple policies on CMS, refer to [Support multiple policies with CMS and shared licensing](#).

For more information on defining a policy, refer to SMA 12.4 Administration Guide.

4. When you are finished defining a policy, click **Save** or **OK**.

Synchronize

To synchronize a policy:

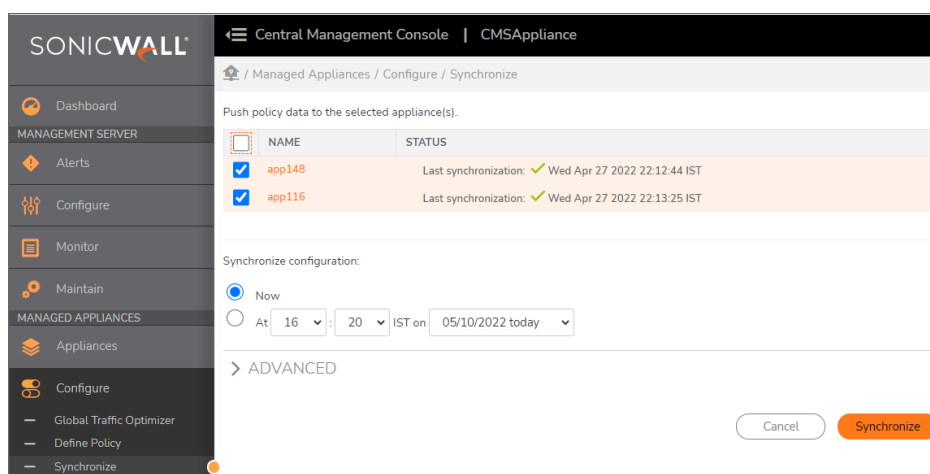
1. Navigate to **Managed Appliances > Configure**.
2. Click **Synchronize**.

3. Click **Advanced** to open the **Advanced** panel.
4. Select **Force selected appliance to import the CMS policy** if you want to reset the appliance policy to the baseline CMS policy.

This triggers the next synchronization (or scheduled synchronization) to overwrite the policies of the selected appliances with the CMS policy, including all custom-defined address pools and authentication servers.

5. Select **Now** if you want to synchronize immediately, or select **At** and choose the time and date from the drop-down menus to schedule the synchronization.
6. Click **Synchronize**.

Synchronizing a policy does not usually terminate existing user sessions. If a synchronization does terminate any user sessions, a warning message is displayed for that appliance on the **Synchronize** page.



Support multiple policies with CMS and shared licensing

CMS multiple policies are all about supporting multiple groups of users under one CMS.

Each group of users can:

- Access a different GTO service
- Have policy elements specific to that group of users
- Use the shared user licenses of the CMS

In the previous versions, CMS was designed for a single policy and a single GTO service. The system is modified as follows:

- Support CMS-based configuration of appliance-specific authentication servers.
- Allow realms and access rules to be mapped to individual appliances.
- Support more than one GTO service, and assign GTO services to one or more appliances.
- Map GTO resources (WorkPlace sites, host-mapped resources) to one or more GTO services.

The goal of this feature is to support remote access geared towards a subset of users under a single company, for example, employees vs partners, or different divisions joined together via M&A.

Other areas of policy and system configuration will remain global and shared across all appliances and GTO services.

License usage in the system will continue to be tracked on a global basis.

Topics:

- [Applying authentication servers to specific appliance](#)
- [Applying SMTP configuration service to specific appliance](#)
- [Applying SMS service to specific appliance](#)
- [Applying realms to a subset of appliance](#)
- [Assign rules to a subset of appliances](#)
- [Support multiple GTO services](#)

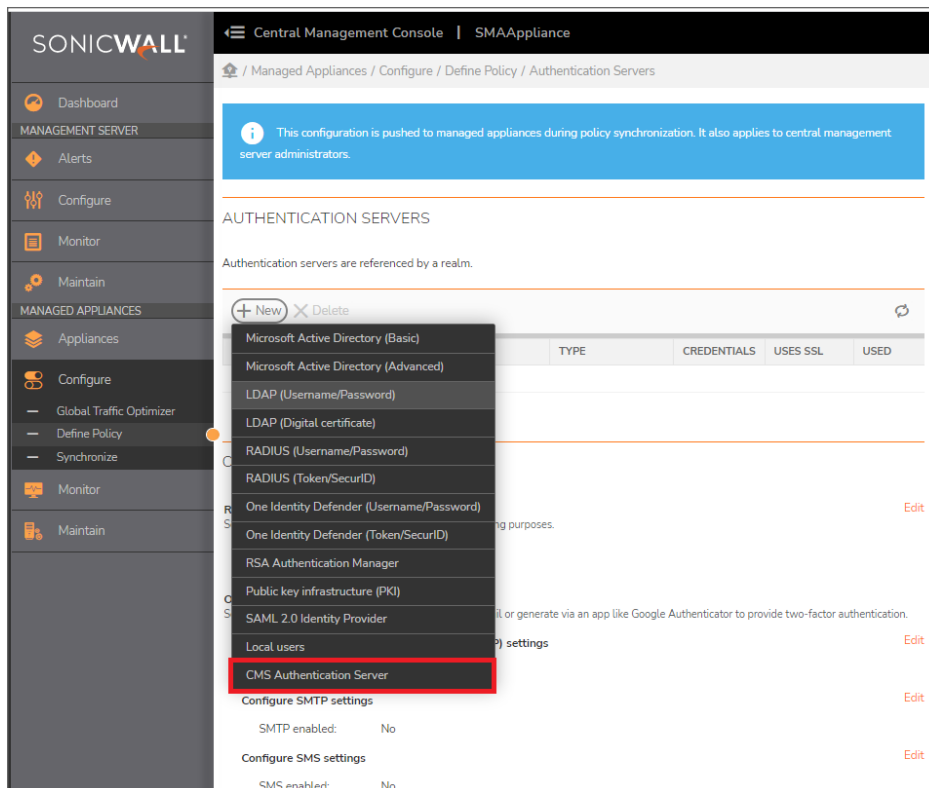
Applying authentication servers to specific appliance

Prerequisites:

- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To enable authentication server specific to appliance:

1. Login to CMS.
2. Navigate to **Managed Appliances > Configure**.
3. Click **Define Policy**.
4. Under **System Configuration**, select **Authentication Servers**.
5. Click **+New**.
6. Select **CMS Authentication Server** as Authentication directory to create a Authentication server.



① **NOTE:** CMS Authentication Server requires that all the authentication servers it maps to must be of the same type. For example, it can map a different AD authentication server configuration to different appliances, but it cannot map one appliance to AD and another to other authentication.

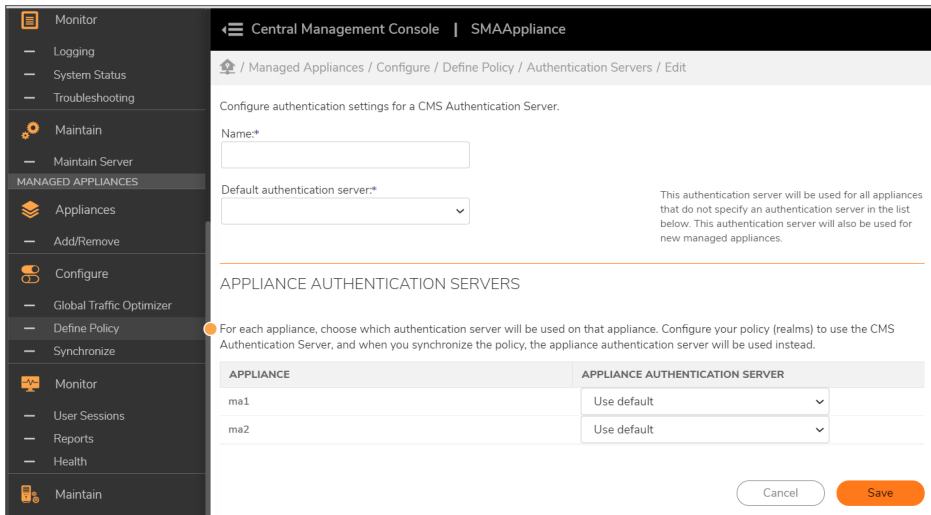
7. Enter the **Name** and select the **Default Authentication Server**.

① **NOTE:** Not all authentication server types can be mapped. For example, local authentication is already shared across the cluster, so it cannot be mapped to an appliance in a CMS authentication server.

8. In the **Appliance Authentication Server**, select the required authentication server to be mapped.

By default, the **Use default** option is set to all the appliance, like CMS address pools, a CMS authentication server has a default authentication server, then 0 or more appliances are mapped to other authentication servers of the same type.

9. Click **Save** and apply pending changes.



10. Proceed to synchronize policy.

The Authentication server assigned to the specific appliance are enabled. The unassigned authentication servers are disabled after policy synchronization from CMS.

NOTE: During policy synchronization, the mapped appliance authentication server (or default if there is no mapping) is replaced in the appliance configuration.

NOTE:

- A CMS authentication server that is being used by a realm cannot be deleted.
- A non-CMS authentication server that is being used by a CMS authentication server cannot be deleted.
- A CMS authentication server can be a primary or secondary authentication server as long as the underlying authentication server type supports it.

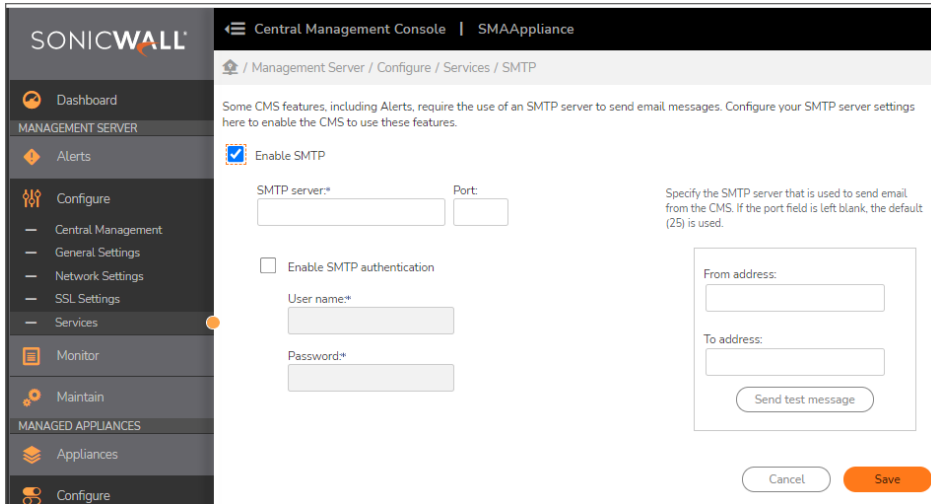
Applying SMTP configuration service to specific appliance

Prerequisites:

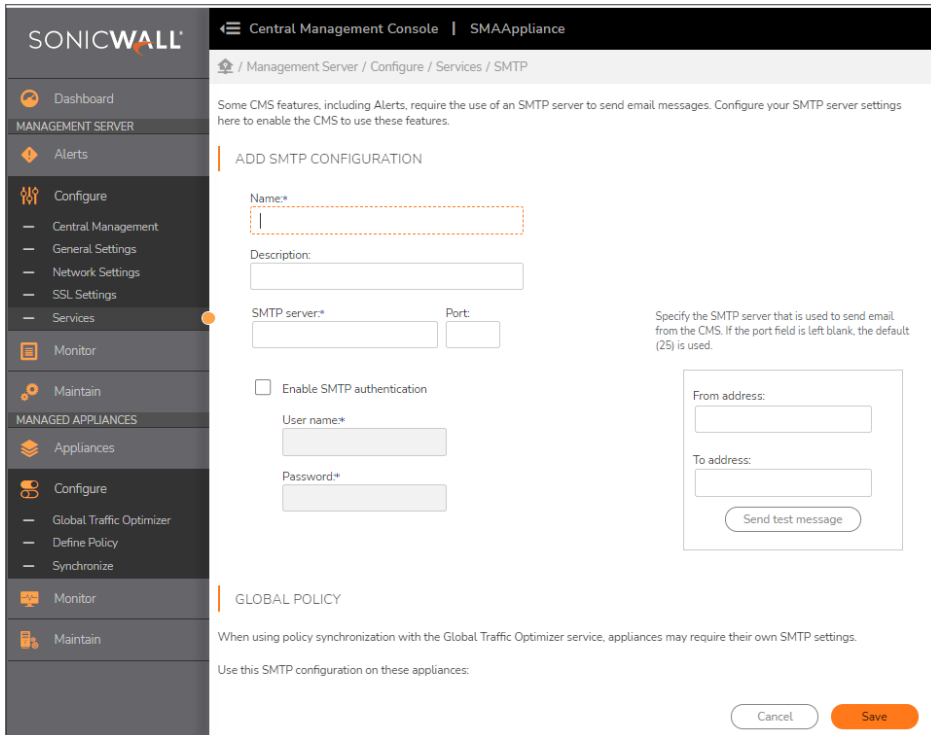
- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To enable SMTP service specific to appliance:

1. Login to CMS.
2. Navigate to **Management Server > Configure**.
3. Click **Services**.
4. Under **SMTP**, click **Configure**.
5. Select the **Enable SMTP** checkbox.
6. Enter the **SMTP server** and **Port** details and click **Save**.



7. Under **Global Policy**, click **+New**.
 ⓘ | **NOTE:** Only 10 SMTP configurations are allowed to be created.
8. Configure the **Add SMTP Configuration**, by entering the **Name**, **Description**, **SMTP Server** and **Port**.
9. Select the **Enable SMTP authentication** checkbox and provide the credentials.



10. Under **Global Policy**, select the SMTP configuration to be used on the appliance.

① **NOTE:** Only one SMTP configuration can be assigned to each of the appliance and Mapping an appliance to an SMTP configuration is automatically unmap it from all other SMTP configurations.

GLOBAL POLICY

When using policy synchronization with the Global Traffic Optimizer service, appliances may require their own SMTP settings.

Use this SMTP configuration on these appliances:

app119

Cancel Save

11. Click **Save** and apply pending changes.

12. Proceed to synchronize policy.

The SMTP configuration is assigned to specific appliance.

① **NOTE:** If an appliance does not have an SMTP configuration mapped to it, it will use the default settings to assign to appliance.

Applying SMS service to specific appliance

Prerequisites:

- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To enable SMS service specific to appliance:

1. Login to CMS.

2. Navigate to **Management Server > Configure**.

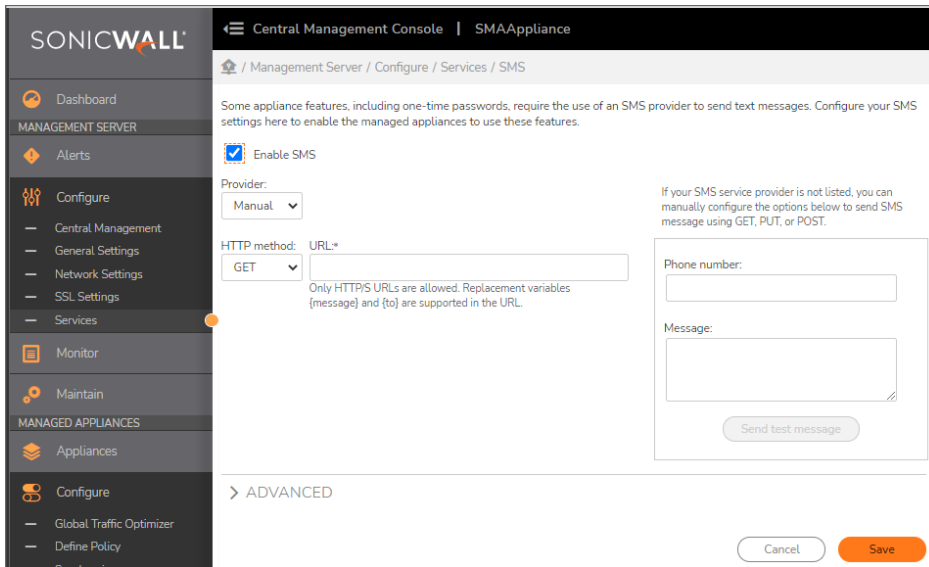
3. Click **Services**.

4. Under **SMS**, click **Configure**.

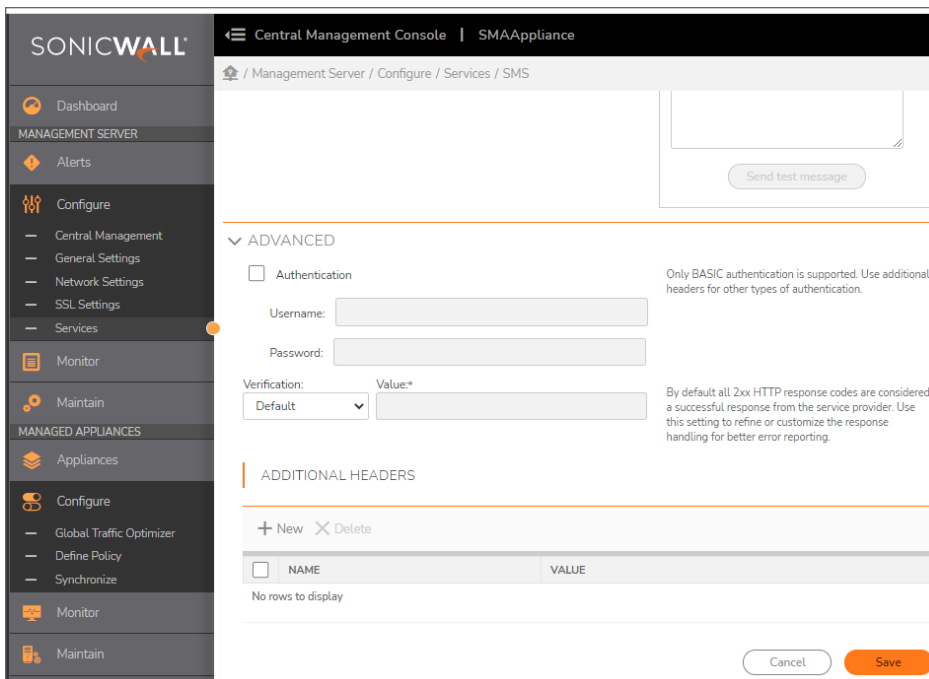
5. Select the **Enable SMS** checkbox.

① **NOTE:** Only 10 SMS configurations are allowed to be created.

6. Configure the SMS settings by selecting the **Provider**, **HTTP Method**, and enter the **URL**.



7. In **Advanced** section, configure the SMS settings.



8. Under **Global Policy**, select the SMS configuration to be used on the appliance.

NOTE: Only one SMS configuration can be assigned to each of the appliance and Mapping an appliance to an SMS configuration is automatically unmap it from all other SMS configurations.

GLOBAL POLICY

When using policy synchronization with the Global Traffic Optimizer service, appliances may require their own SMS settings.

+ New × Delete

<input type="checkbox"/>	NAME	DESCRIPTION	SMS PROVIDER	APPLIANCES
<input type="checkbox"/>	sms1_pvelan		Custom: https://sms.com	None
<input type="checkbox"/>	sms2		Custom: https://sms2.com	None
<input type="checkbox"/>	sms3		Custom: https://sms.com	None
<input type="checkbox"/>	sms4		Custom: https://sms.com	None
<input type="checkbox"/>	sms5		Custom: https://sms2.com	None
<input type="checkbox"/>	sms6		Custom: https://sms.com	None
<input type="checkbox"/>	sms7		Custom: https://sms.com	None
<input type="checkbox"/>	sms8		Custom: https://sms.com	None
<input type="checkbox"/>	sms9		Custom: https://sms.com	None

9. Click **Save** and apply pending changes.

10. Proceed to synchronize policy.

The SMS configuration is assigned to specific appliance.

NOTE: If an appliance does not have an SMS configuration mapped to it, use the default settings to assign to appliance.

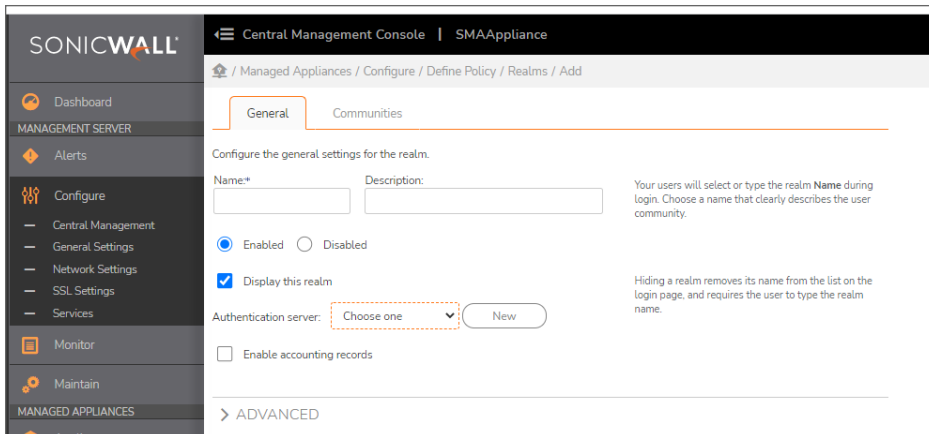
Applying realms to a subset of appliance

Prerequisites:

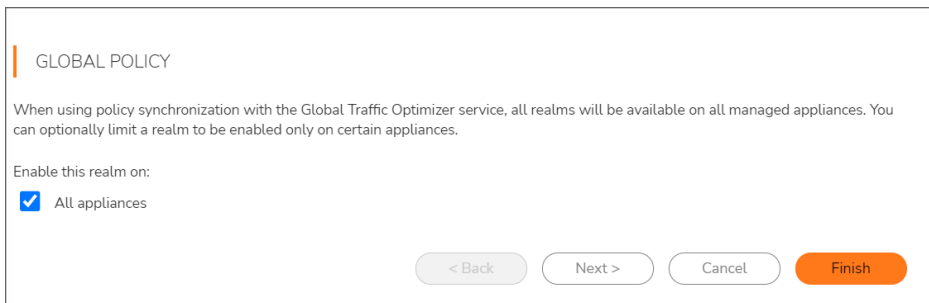
- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To enable realms to be a subset of appliance:

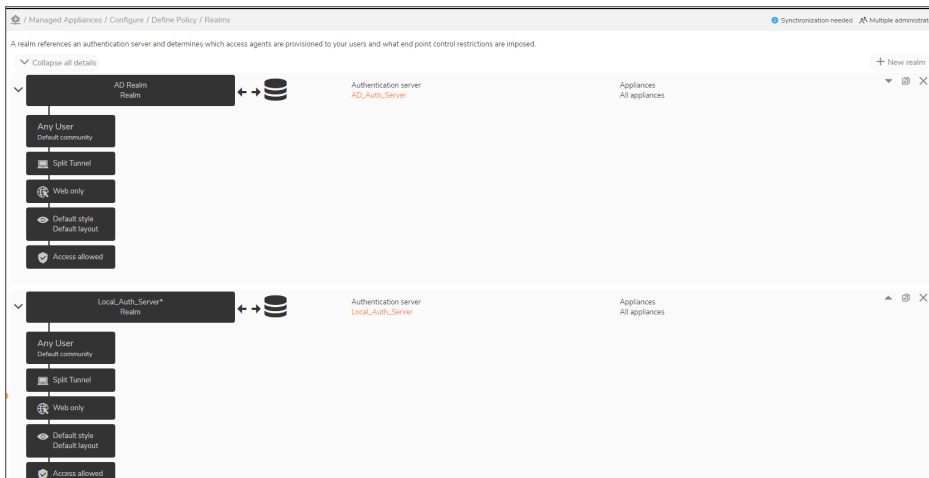
1. Login to CMS.
2. Navigate to **Managed Appliances > Configure**.
3. Click **Define Policy**.
4. Under **User Access**, select **Realms**.
5. Click **+New**.
6. Configure the realm settings by entering the **Name**, **Description**, and select the **Authentication server**.



7. Under **Global Policy**, select the realm to a subset of appliance.
 ⓘ | **NOTE:** The default will be to expose all realms on all appliances.
8. Click **Finish** and apply changes.



9. Proceed to synchronize policy.
 The realms view contains label displaying all the appliances assigned with the realms.



NOTE:

- Unmapped realms will not be removed from the policy during synchronization with the managed appliance, but will be disabled and will not be visible to clients.
- There will be no changes on AMC User Interface (UI). Appliances will not know that they are running with the appliance-specific realms.

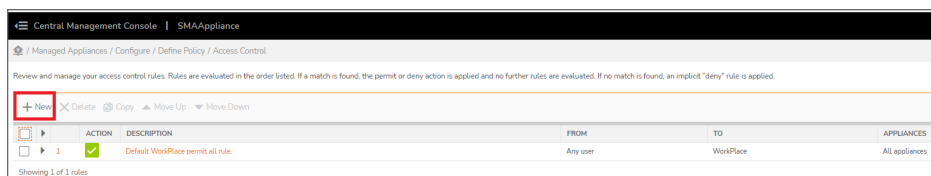
Assign rules to a subset of appliances

Prerequisites:

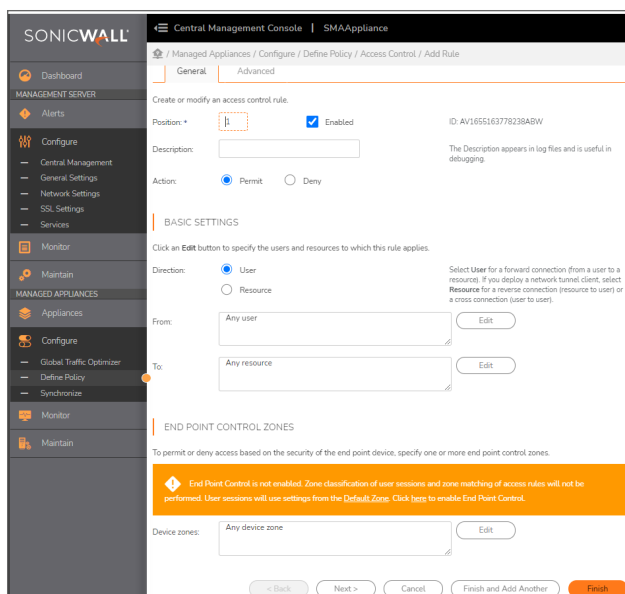
- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To assign rules to a subset of appliance:

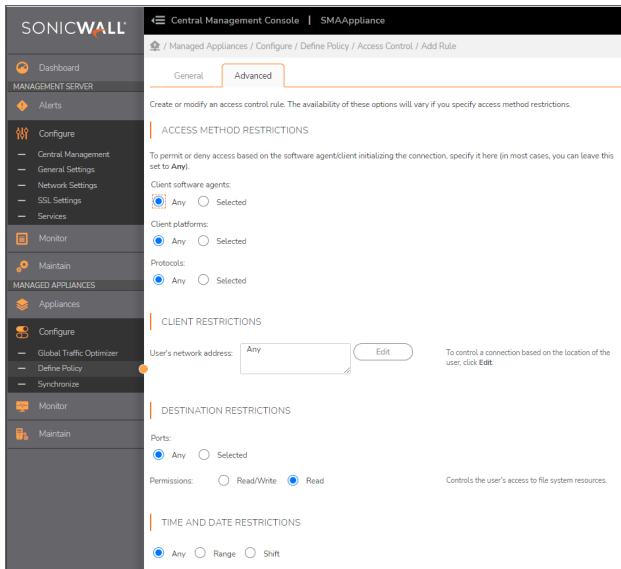
1. Login to CMS.
2. Navigate to **Managed Appliances > Configure**.
3. Click **Define Policy**.
4. Under **Security Administration**, select **Access Control**.
5. Click **+New**.



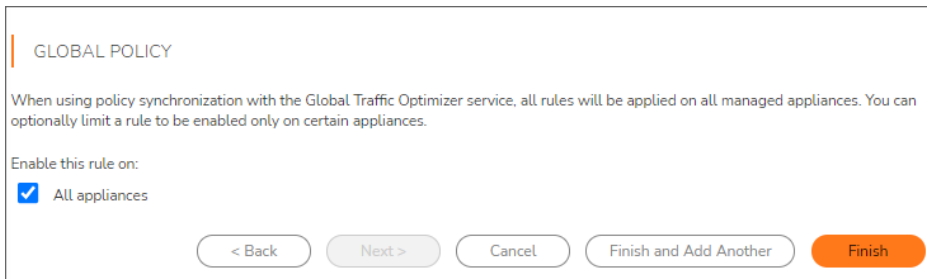
6. In **General** tab, configure to add a new rule and click **Next**.



7. In **Advanced** tab, configure the required settings.



8. Under **Global Policy**, select the realm to assign rules to specific appliances.
9. Click **Finish** and apply changes.



10. Proceed to synchronize policy.
All the appliances are assigned with the rules.

NOTE:

- Unmapped rules will not be removed from the policy during synchronization with the managed appliance, but they will be disabled so they will not have any affect.
- No changes on AMC UI, appliances will not know that they are running with the appliance-specific rules.

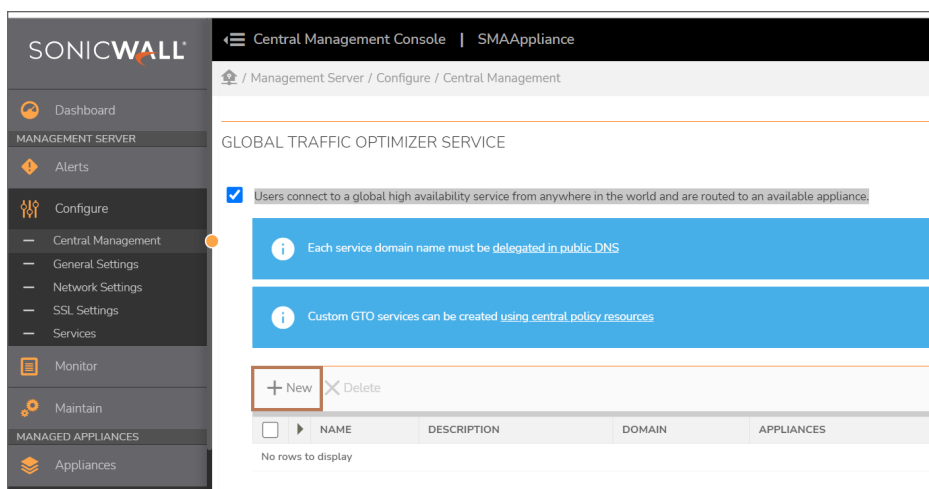
Support multiple GTO services

Prerequisites:

- SMA1000 CMS and minimum two managed appliances running firmware version 12.4.

To support multiple GTO services:

1. Login to CMS.
2. Navigate to **Management server > Configure > Central Management**.
3. Select **Users connect to a global high availability service from anywhere in the world and are routed to an available appliance under Global Traffic Optimizer Service**.
4. Click **+New**.



NOTE: Only 10 GTO services can be configured on CMS.

5. Configure top-level GTO service and assign it to one or more appliances.
 - NOTE:** If a GTO service is not assigned to any appliance, it will be assigned for all appliances. There is no relationship between the appliances that are configured as authoritative name servers and the way in which GTO services are mapped to appliances.
6. Click **Save** and apply pending changes.

ADD GTO SERVICE

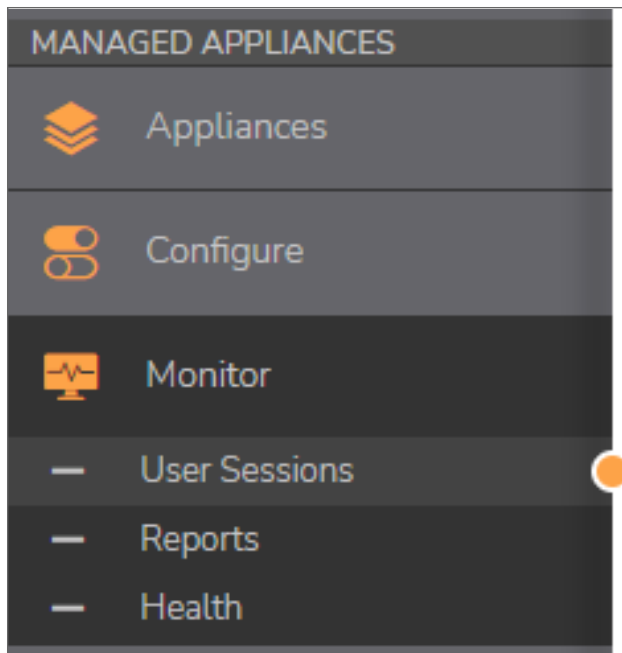
Name: <input style="width: 90%; border: 1px dashed orange;" type="text"/>	Name of this GTO service
Description: <input style="width: 90%;" type="text"/>	Description of this GTO service
Service domain: <input style="width: 90%;" type="text"/> Example: access.example.com	Domain name of this GTO service
Enable this GTO service on: <input checked="" type="checkbox"/> All appliances	
<input type="button" value="Cancel"/> <input style="background-color: #f4a460; border: none; padding: 5px 15px;" type="button" value="Save"/>	

7. Proceed to synchronize policy.
The GTO services are mapped to appliances.

- NOTE:**
- Generated Let's Encrypt certificates will include FQDNs for all top-level services and auto-generated services for all applicable appliances.
 - There is no change to AMC.
 - The GTO resources that are automatically generated based on resources and WorkPlace sites are mapped to appliances based on the top-level GTO service that they match.

Monitor

The Monitor option for Managed appliances provides detailed information on **User Sessions, Reports** and **Health**. Select **Managed Appliances > Monitor** to see the options.



Topics:

- [User Sessions](#)
- [Reports](#)
- [Health](#)

User Sessions

On the **User Sessions** page, you can view current and past user sessions and terminate current sessions. If you select a session and then select the **Terminate session-restrict logins** option, it temporarily disables the user's access for up to 10 minutes.

To monitor user sessions:

1. Navigate to **Managed Appliances > Monitor**.
2. Click **User Sessions**.
3. Define how the data needs to be appear in the table:
 - a. In the **View** field, select the number of users to show per page.
 - b. In the **Sessions** field select the type of session to view: **Licensed**, **All open**, or **All**.
 - c. From the drop-down menus under Filters, select the items you want to view or manage.
4. If you want to filter the data further, select options from the drop down lists under **Appliance**, **Login**

status, Realm, Community, Zone, Agent, and Platform.

Managed Appliances / Monitor / User Sessions SSL warning

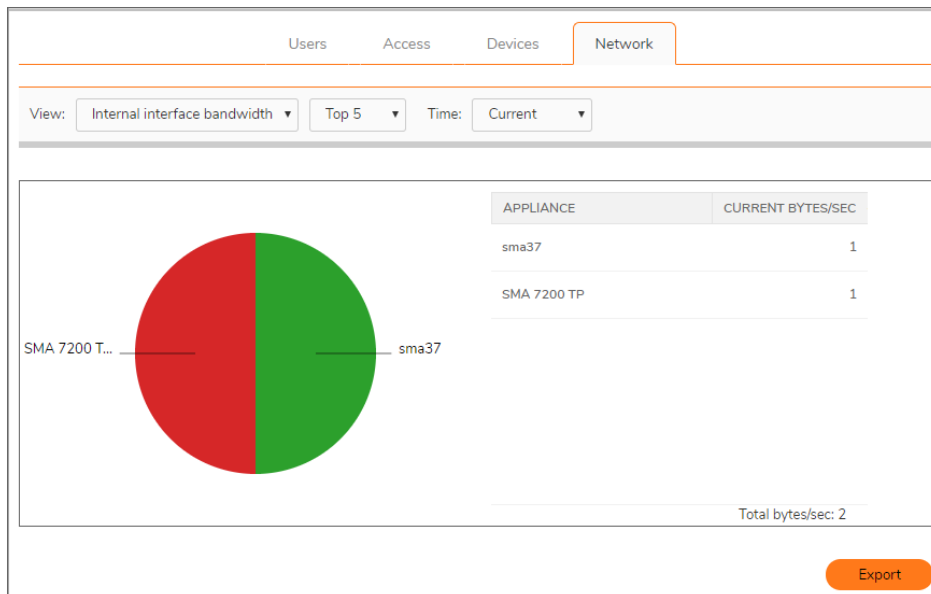
View current and past user sessions and terminate current sessions. Using the restrict logins option will temporarily disable a user's access for 10 minutes.

Terminate session Restrict logins Export View: 50 Sessions: Licensed Time period: Current

	USER	APPLIANCE	STARTED	ENDED	ELAPSED	AVG BYTES/MIN	TOTAL BYTES
<input type="checkbox"/>	user1001@qaperf.local	app223.perfapp-223	07/06/2022 06:29 IST		0 days, 2:03	7.66 MB	547 MB
<input type="checkbox"/>	user1002@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.33 GB
<input type="checkbox"/>	user1004@qaperf.local	app202.SMAApliance	07/06/2022 06:30 IST		0 days, 2:03	16.3 MB	1.63 GB
<input type="checkbox"/>	user1004@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.36 GB
<input type="checkbox"/>	user1005@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.33 GB
<input type="checkbox"/>	user1006@qaperf.local	app223.perfapp-223	07/06/2022 06:30 IST		0 days, 2:02	7.94 MB	626 MB
<input type="checkbox"/>	user1009@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.37 GB
<input type="checkbox"/>	user1009@qaperf.local	app07.perfapp-97	07/06/2022 06:30 IST		0 days, 2:02	11.6 MB	1.20 GB
<input type="checkbox"/>	user1009@qaperf.local	app202.SMAApliance	07/06/2022 07:47 IST		0 days, 2:46	6.60 MB	1.33 GB
<input type="checkbox"/>	user1009@qaperf.local	app223.perfapp-223	07/06/2022 04:36 IST		0 days, 6:56		3.80 GB
<input type="checkbox"/>	user1010@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.30 GB
<input type="checkbox"/>	user1011@qaperf.local	app111.SMAApliance	07/06/2022 06:30 IST		0 days, 2:02	7.72 MB	604 MB
<input type="checkbox"/>	user1011@qaperf.local	app202.SMAApliance	07/06/2022 04:50 IST		0 days, 6:42		1.36 GB
<input type="checkbox"/>	user1014@qaperf.local	app111.SMAApliance	07/06/2022 06:30 IST		0 days, 2:02	7.86 MB	795 MB
<input type="checkbox"/>	user1015@qaperf.local	app223.perfapp-223	07/06/2022 04:50 IST		0 days, 6:42		1.65 GB
<input type="checkbox"/>	user1019@qaperf.local	app111.SMAApliance	07/06/2022 06:30 IST		0 days, 2:02	7.71 MB	617 MB
<input type="checkbox"/>	user1019@qaperf.local	app07.perfapp-97	07/06/2022 06:31 IST		0 days, 2:01	11.7 MB	1.23 GB
<input type="checkbox"/>	user1019@qaperf.local	app223.perfapp-223	07/06/2022 04:50 IST		0 days, 6:42		1.73 GB

Reports

On the **Reports** page, you can view reports about Users, Access, Devices, and the Network.



- **User** — View reports that show the number of user sessions on appliances or realms, for example, the number of user sessions currently on selected appliances, or the count for each of the top five realms of licensed users for the last day.
- **Access** — View reports that show the policy rules matched and destinations accessed by users on managed appliances, for example, the top five permit rules and how many times they have been enforced over the last hour, or the count for each of the top five most accessed destinations over the last day.

- **Devices** — View reports that show the platforms and zones in use by users, for example, a user's platform distribution for the last week, or a user's zone placement count for the last month.
- **Network** — View reports on the bandwidth consumption of appliances and the data transferred to users. For example, the top five users who transferred the most data and how much they transferred over the last hour or over the last three months, or view the top five appliances that consume the most bandwidth and how much they are currently consuming.

To view the reports:

1. Select the category: **Users**, **Access**, **Devices**, or the **Network**.
2. From the drop down lists, select the options for **View**.
 ⓘ | **NOTE:** The option for the View fields vary according to the type of report selected.
3. Select an option from the Time drop down list.
 The display adjusts according to the selections made. Select **Refresh** to refresh the data in the report. Select **Export** to export the data to a CSV file.

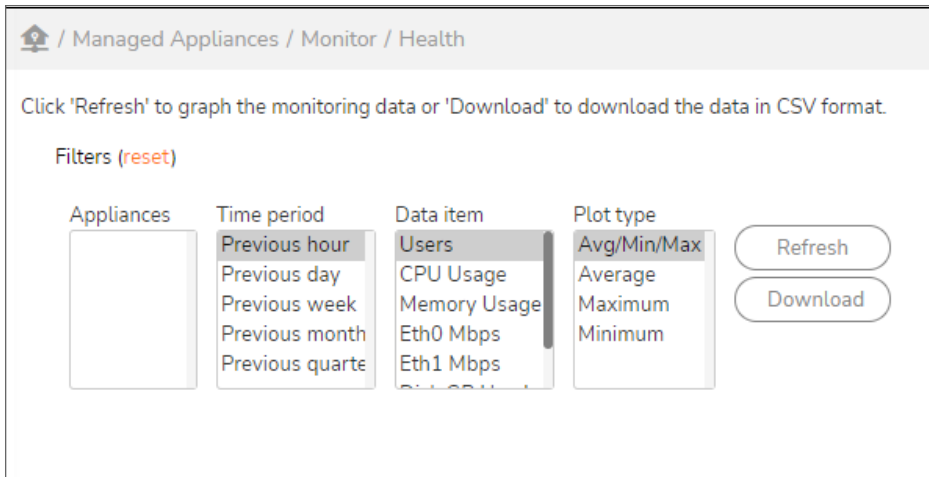
Health

On the **Health** page, you can set up and monitor various health metrics on a graph that charts users against time. The data is downloadable to a CSV file.

To monitor health metrics:

1. Navigate to **Managed Appliances > Monitor**.
2. Click **Health**.
3. From the **Appliances** menu, select the appliance you want to graph.
4. From the **Time period** menu, select the time period you want the graph to display.
5. From the **Data item** menu, select the data you want the graph to display.
6. From the **Plot type** menu, select the type of graph you want to plot.

7. Select **Refresh** to refresh the data or select **Download** to download the data to a CSV file.



Maintain

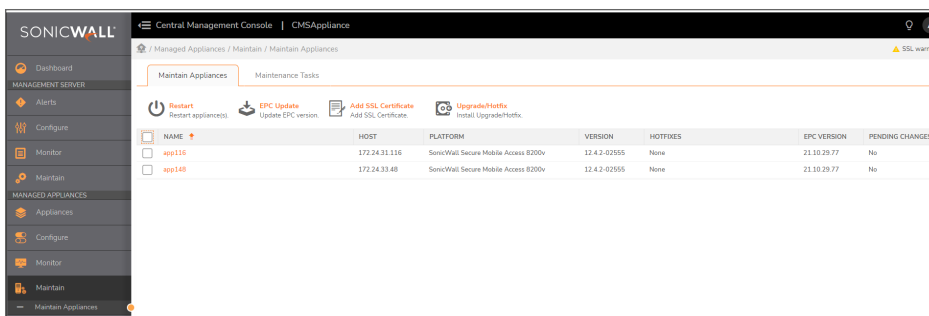
Navigate to **Managed Appliances > Maintain**. This page has two options:

- Maintain Appliances
- Maintenance Tasks

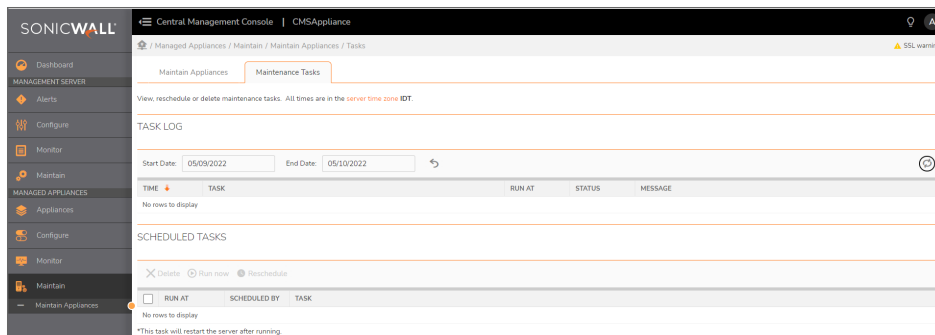
Maintain Appliances

To maintain a managed appliance:

1. Navigate to **Managed Appliances > Maintain**.
2. Click the **Maintain Appliances**.
3. Check the box for an appliance and use the buttons across the top to perform any of the following tasks: **Restart**, **EPC Update**, **Add SSL Certificate**, **Upgrade/Hotfix**.



Maintenance Tasks



Viewing Maintenance Tasks

To view maintenance tasks:

1. Navigate to **Managed Appliances > Maintain**.
2. Click the **Maintenance Tasks** tab.
The Task Log lists recent and upcoming maintenance tasks.


Deleting Scheduled Maintenance Tasks

To delete scheduled maintenance tasks:

1. Navigate to **Managed Appliances > Maintain**.
2. Click the **Maintenance Tasks** tab.
The Task Log lists recent and upcoming maintenance tasks.
3. In the **Scheduled Tasks** section, select the maintenance tasks you want to cancel.
4. Click the **X** (Delete) icon.


Rescheduling Maintenance Tasks

To cancel re-schedule maintenance tasks:

1. Navigate to **Managed Appliances > Maintain**.
2. Click the **Maintenance Tasks** tab.
The Task Log lists recent and upcoming maintenance tasks.
3. In the **Scheduled Tasks** section, select the maintenance tasks you want to cancel.
4. Click the  (Reschedule) icon.

Performing Maintenance Tasks Immediately

To perform maintenance tasks immediately:

1. Navigate to **Managed Appliances > Maintain**.
2. Click the **Maintenance Tasks** tab.
The Task Log lists recent and upcoming maintenance tasks.
3. In the **Scheduled Tasks** section, select the maintenance tasks you want to cancel.
4. Click the  (Run Now) icon.

Central User Licensing

Topics:

- [Overview](#)
- [How Central User Licenses Work](#)
- [Enabling Central User Licensing](#)
- [Getting Started with Central User Licensing](#)

Overview

Central User Licensing is an optional feature that allows a CMS to share a pool of user licenses among managed appliances. Customers with appliances that are globally distributed can use their licenses more efficiently with central user licenses where user demands peak in one geographic area while it falls in a different geographic area due to off-work/night hours. Appliances that are in a datacenter can share licenses instead of having individual licenses for each appliance. When new or replacement appliances (physical or virtual) are added under CMS management, they get to share the pool of central user licenses.

Central user licensing must be enabled to use Global High Availability.

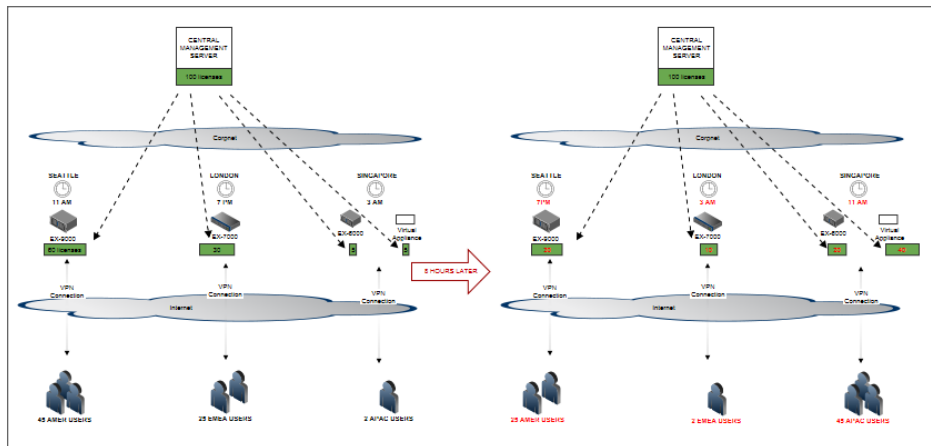
① **NOTE:** If CMS is used to manage appliances that have their own license, the administrator is responsible for ensuring that licenses across all managed appliances have the same features. CMS cannot manage configurations on appliances with a heterogeneous set of licensed features.

How Central User Licenses Work

User licenses do not have to be applied to individual VPN appliances. The pooled licensing model allows central user licenses to be shared among the managed appliances. Central user licensing makes use of a distributed data store to keep track of license usage. The distributed data store has storage nodes on multiple appliances so that central user licensing is resilient to the failure of (or communication loss with) the CMS or any one appliance.

- ① **NOTE:** Managed appliances must be able to communicate with each other via their external interface IP addresses or internet-routable IP addresses in order for them to be able to share information in the distributed data store.

The following drawing illustrates centrally managed licenses for globally located VPN appliances.



- ① **NOTE:** Beginning with the SMA 12.1 release, CMS uses a distributed data store to track user license consumption for each appliance and to regulate the total number of pooled user licenses being used.

In the event of a **CMS failure (or loss of communication)**:

- Managed appliances will continue to access the distributed data store and share central user licenses.

In the event **an appliance is orphaned (unable to communicate with the CMS or other appliances)**:

- An orphaned appliance will have access to the all the central user licenses (and spike licenses) for 7 days or until communications are re-established.

In the event of a **communication loss between the CMS and MySonicWall**:

- The central user licenses continue to be valid for 30 days.

Topics:

- [Central Spike User Licenses](#)
- [Central Email Licenses](#)
- [Perpetual Pooled Licenses](#)

Central Spike User Licenses

Spike licensing allows temporary increases in the number of available licenses to meet sudden increases in demand for licenses due to inclement weather or disaster. Spike licenses can be applied to a CMS using either a subscription user license or perpetual user license. Spike user licenses are “full” user licenses and allow any type of connection (e.g., tunnel, web, ActiveSync). A spike license is automatically activated for a day if the user session count exceeds the CMS user license count.

When a spike is active, it allows the appliances to service up to sum of:

- the CMS base license max user count
- the spike license max user count

The CMS Dashboard and Licensing page will indicate that a spike is in effect, along with its Start and Stop times.

A central spike license allows any of these user licenses to spike:

- Subscription full-user license
- Subscription tiered-user license
- Perpetual full-user license

① | **NOTE:** When a spike license is installed on a CMS with a subscription user license, and the subscription license expires, the spike will remain enabled.

① | **NOTE:** When SMA is licensed with a standalone license, and that license expires, the spike license also expires.

The CMS administrator can control whether or not to use automatic spike licensing.

Central Email Licenses

Different terms for central email licensing are available:

Full license Permits a connection of any of these connection types: - VPN tunnel, web, ActiveSync, or Outlook Anywhere

Email license A license that permits an ActiveSync or Outlook Anywhere connection

Depending on which licensing terms are available for the appliance, licensing for email connections will be applied in this way:

- During operation, if an ActiveSync connection request is made and Email licenses are available, then an Email license will be used.
- If all Email licenses are consumed and an ActiveSync connection request is made (and full licenses are available), then a full license will be used.
- The license that is issued when a connection begins will remain with the connection until it ends.

Perpetual Pooled Licenses

Perpetual pooled licenses are CMS-based user licenses that do not expire in the way that subscription-based licenses do:

- Perpetual licenses are full user licenses and allow any type of connection (e.g., tunnel, web, ActiveSync).
- Perpetual CMS licenses are stackable. Licenses remains perpetual after being stacked.

① | **NOTE:** Perpetual CMS user licenses cannot be stacked with a subscription CMS user license.

These licenses and components can be used with a perpetual pooled license:

- Subscription email license
- Subscription Capture CMS license
- Time-limited subscription components

Enabling Central User Licensing

To enable Central User Licensing on the CMS:

1. Navigate to **Management Server > Configure**.
2. Click **Central Management**.
3. Under **Central User Licensing**, select **Enable managing appliance user licensing with one central license**.
4. Click **Save**.

The screenshot shows the configuration page for Central Management. The breadcrumb trail is: / Management Server / Configure / Central Management. Below the breadcrumb, there is a descriptive text: "This central management server manages the licensing and configuration for a collection of appliances." The page is divided into sections by horizontal lines. The first section is titled "LOCALE" and contains two fields: "Country or region:" with a dropdown menu showing "N/A", and "Location:" with a text input field. Below the "Location:" field is an example: "Example: Seattle, WA". The second section is titled "CENTRAL USER LICENSING" and contains a checked checkbox with the text: "Enable central user licensing. The current CMS license will support 50 users and 50 email users across all appliances".

Getting Started with Central User Licensing

This section describes how to migrate from a standalone appliance to CMS with Global HA and Central User Licenses.

Topics:

- [Setting Up CMS to Use Central User Licenses](#)
- [Setting up CMS for Centralized Appliance Configuration and Management](#)
- [Resetting a CMS License](#)

Setting Up CMS to Use Central User Licenses

Once you have SMA appliances registered with CMS, you can transition to Central User Licensing.

① | **NOTE:** If you have an HA Pair, you need to engage with SonicWall Sales to exchange your HA pair licenses for CMS-based Central User Licenses.

To transition standalone SMA appliances to use the Central User License model:

1. Log into the Central Management Console.
2. Navigate to **Management Server > Configure > General Settings**.
3. Under **Licensing**, click **Edit**.
The **Manage Licenses** page displays.
4. Select **Register**.
5. Enter the MySonicWall credentials of the MySonicWall account who owns the licenses for the Central Management Server.
6. Enter the serial number and authentication code that match the license in MySonicWall.
7. Enter a friendly name to identify this CMS in your MySonicWall account.
8. Select **Submit**. You see the MySonicWall view of your license.
You can get back to this at any time after you are registered by navigating to **Management Server > Configure > General Settings** and clicking on **Licensing > Edit** and re-entering your MySonicWall credentials.
9. Select **Return**. This is the normal view of a registered CMS license. It shows the licensing mode as online and how long since it was last synchronized. It should never be more than 24 hours since the last synchronization.

① | **NOTE:** You can also select Synchronize to force an immediate synchronization with MySonicWall.

Setting up CMS for Centralized Appliance Configuration and Management

Once you have a cluster of SMA appliances that share a central license pool and you can monitor and maintain them from a single console.

If your appliances have very different configurations, you should normalize the differences so that you can take full advantage of CMS, GTO, and Global HA.

To use CMS to centralize appliance configuration management:

1. Normalize the appliance configurations.
2. Export the configuration from your SMA appliance.
3. Import the configuration to CMS.

4. Synchronize the CMS policy with the managed appliances.
5. Configure the CMS as described in [Configure](#).

Resetting a CMS License

The license state on a Central Management Server can be reset or undone.

1. Navigate to the **Licensing** page.
2. Add `?troubleshoot=1`.
3. Select **Reset**.

This reboots the CMS with no license and it can be registered again with MySonicWall.

Global High Availability

Global High Availability (Global HA) facilitates global high availability with load distribution and disaster recovery capabilities across the SMA appliances in the GTO service. The high availability can be deployed in a single datacenter or across dispersed data centers.

Topics:

- [High Availability of the VPN Service](#)
- [High Availability of the CMS](#)
- [Disaster Recovery for the VPN Service](#)

NOTE: Global High Availability replaces the HA Pair model. Secure Mobile Access version 11.4 is the last version of SMA that supports HA Pairs. See the Comparison of HA Pair and GTO with Global HA table for a comparison of the two models.

High Availability of the VPN Service

Global High Availability (Global HA) is configured from the CMS console by first enabling the Global Traffic Optimizer (GTO) service. Users access the VPN using the service name (e.g. `access.example.com`) in the VPN tunnel clients (Connect Tunnel or Mobile Connect) or the web client. The GTO service directs user connections to an appliance that is available.

Global HA enables SMA appliances to scale performance by deploying multiple appliances under a service name. Global HA eliminates a single point of failure and provides a highly available global VPN service. Customers can deploy 2 SMA appliances in the same data center or across multiple data centers around the globe.

A distributed data store shares user session state as well as licensing information across the mesh network of SMA appliances. This allows for session persistence across appliances. In the event of a failover, users are connected to another appliance in the service. The distributed data store also allows for central user licenses to be shared across appliances and data centers.

All of the SMA appliances that are configured for the GTO service participate in the highly available VPN service. If an appliance that is part of the service fails due to hardware, power, or network issues:

- New connection requests (by tunnel or web clients) will get directed to other available appliances.
- Existing connections (that were connected to the appliance that failed) are automatically reconnected to another available appliance. Users typically do not need to re-enter their credentials.

High Availability of the CMS

Customers can setup their CMS in a virtual infrastructure (ESXi, Hyper-V, AWS, Azure, or KVM) that supports high availability. The following HA models can be used to enable a fault tolerant CMS.

CMS HIGH AVAILABILITY AND DISASTER RECOVERY FEATURES

CMS Global HA and Disaster Recovery Scenarios	VMware ESXi / Microsoft Hyper-V/ AWS /Azure / KVM	Comments
HA Clustering	Yes	Seamless transition of CMS in a HA cluster from host 1 to host 2, when host 1 is rebooted or shutdown
Cloning of CMS	Yes	CMS can be successfully cloned followed by resumption of communication with managed appliances and the License Manager service
Export/Import	Yes	CMS could be successfully exported from host 1 and imported to host 2 followed by resumption of communication with managed appliances and the License Manager service.
Snapshot/Checkpoint	Yes	Successful preservation and transition

Disaster Recovery for the VPN Service

Customers can setup Disaster Recovery (DR) for their VPN by locating appliances that are in a Global Traffic Optimizer (GTO) service at different data centers.

Disaster recovery of the VPN service enables the continuation of remote access capabilities when a disaster or failure occurs to a major location. Users use the same GTO service name (such as access.example.com) and SMA appliances that are located at other locations that are part of the global VPN service accepts the connection requests.

Planning the Disaster Recovery for the VPN service is done in conjunction with disaster recovery planning of other essential IT services. SMA appliances (that are part of the GTO service) must be located at alternate data centers along with other key infrastructure components.

If a disaster destroys a data center that has SMA appliances, the remaining appliances continue to provide service.

Alerts and SNMP

It consists of the following topics:

Topics:

- [Overview](#)
- [Pre-Configured Alerts](#)
- [Configuring SNMP](#)

Overview

This section contains detailed information about alerts and the use of SNMP in the CMS.


The CMS generates alerts that are either Warnings or Errors. Alerts are displayed prominently on the CMS dashboard. Alerts can originate from a condition that occurs on the CMS, or from a managed appliance.

Alerts can be configured to generate SNMP traps that are monitored by any IT infrastructure Network Management System (NMS).

Pre-Configured Alerts

The Table of Pre-Configured Alerts below has a fixed set of conditions that can trigger alerts.



NOTE: The Priority symbols represent a Warning  or an Error .

The administrator can edit the pre-configured alerts as follows:

- Modify or customize these pre-configured default alerts.
- Disable them
- Make changes to the threshold, duration and message.
- Configure additional alerts. The Table of Alerts lists all the conditions that can be used to configure Alerts.
- Configure the priority of an alert to either Critical or Warning.
- SNMP traps are generated for all Critical alerts.

For these activities, use the following guidelines:

- When an appliance-related alert is configured, it applies to all the managed appliances, that is, alerts cannot be individually configured/tailored for a specific appliance.
- The maximum number of alerts that can be configured by the administrator on a CMS is 100.

Alerts shown on the dashboard can be dismissed by the administrator. Dismissed alerts will no longer be displayed in the dashboard view, but can be seen in the Alerts page. If the alert condition toggles (ON->OFF->ON), a new alert for the same condition will be raised in the dashboard.

All alerts are stored in the Alerts Database. A rolling history of 90 days worth of alerts are retained in the Alerts Database. An Alerts View allows the administrator to see all Alerts in the past Day, Week, Month or Quarter.

Configuring SNMP

To enable SNMP:

1. Navigate to **Management Server > Configure**.
2. Click **Services**.
3. Under **SNMP**, click **Configure**.
4. Enter the information you want in the appropriate fields.
5. Click **Save** and **Apply Pending Changes**.

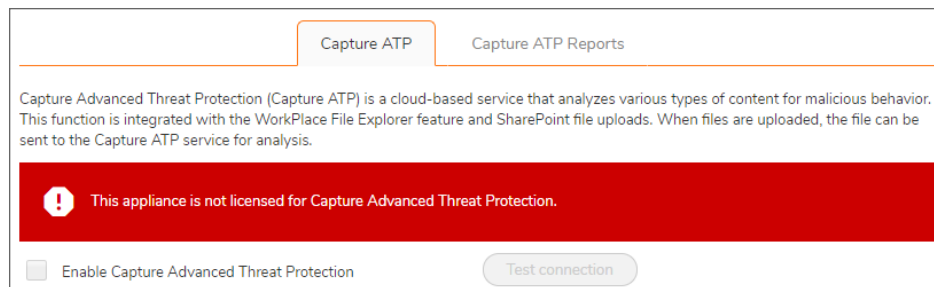
The screenshot shows the 'Configure Simple Network Management Protocol (SNMP)' page. The breadcrumb navigation is 'Management Server / Configure / Services / SNMP'. The page title is 'Configure Simple Network Management Protocol (SNMP). SNMP can be used to manage the CMS and managed appliances.' There is a 'Download MIB' button in the top right. The configuration options include: 'Disable SNMP' (selected with a radio button), 'Enable SNMPv2' (unselected), and 'Enable SNMPv3' (unselected). Below these is an 'Interface selection' dropdown menu set to 'Internal'. The page is divided into sections: 'AGENT PROPERTIES' with fields for 'System location' and 'System contact'; 'SNMPV2 AGENT PROPERTIES' with 'System name' (SMAAppliance) and 'Community string:*' (public); and 'SNMPV3 AGENT PROPERTIES' (partially visible).

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. 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 SMA 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:



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*.

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. Navigate to **Managed Appliances > Configure**.
2. Click on **Define Policy**.
3. In the **User Access** section, click **Capture Advanced Threat Protection**.
The **Capture ATP** page displays.

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.

Network Tunnel Service
Manages TCP/IP connections from the network tunnel clients (Connect Tunnel and OnDemand Tunnel).

Web Proxy Service
Manages HTTP and TCP/IP connections from web browsers, OnDemand, and Connect Tunnel.

WorkPlace
Manage workplace shortcuts, shortcut groups, sites, appearance, and settings.

SAML Identity Provider
Manages the SAML Identity Provider service.

Agent Configuration
Manage access agents and other agents.

End Point Control
Manage end point control settings.

Capture Advanced Threat Protection
Manage Capture Advanced Threat Protection settings.

4. Select **Enable Capture Advanced Threat Protection**.

Home / Managed Appliances / Configure / Define Policy / Capture ATP

Capture ATP

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 Test connection

5. 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 MB

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. Navigate to **Managed Appliances > Configure**.
2. Click **Define Policy**.
3. In the **User Access** section, select **Capture Advanced Threat Protection**.
The **Capture ATP** page displays.
4. 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.
5. Click **Save**.

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 MB

To set the maximum file size:

1. Navigate to **Managed Appliances > Configure**.
2. Click **Define Policy**.
3. In the **User Access** section, select **Capture Advanced Threat Protection**.

The **Capture ATP** page displays.

4. 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.
- ① | **NOTE:** The maximum file size supported by SMA 12.4.1 onwards is 50MB.
5. Click **Save**.

Web Services

① | **NOTE:** The resource must be classified as a SharePoint web service for this feature to function. See “Configuring a Resource as a SharePoint Web Service” in the *SMA 12.4 Administration Guide*.

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. Navigate to **Managed Appliances > Configure > Define Policy**.
2. Click **Capture Advanced Threat Protection**.
3. In the **Web Services** section, select **Send SharePoint file uploads to Capture ATP service**.
4. Click the **Save** button.

① | **NOTE:** The restrictions set for Capture ATP for file types and maximum sizes will apply to files uploaded to SharePoint site. See [File Options](#) 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).

Central FIPS Licensing

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 8200v, 7200, 7210, and SMA 6200, 6210 appliances have 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).

FIPS mode is transparent to end users. Internally, FIPS mode enforces secure communication and system integrity.

FIPS can be enabled on centrally managed appliances.

- A central FIPS license allows all appliances managed by the CMS to be FIPS-enabled.
- To be managed by the CMS, FIPS-enabled appliances are not required to be part of a GTO service.
- A CMS license that includes FIPS must also include central user licenses. An appliance that is not centrally licensed, but has its own user license file, cannot be FIPS-enabled from a CMS-based license.

When the CMS central user license has FIPS, the administrator can enable FIPS individually for any managed appliance from its AMC. (See “Enabling FIPS” in the *SMA 12.4 Administration Guide* for more information.)

For more information about FIPS, see “FIPS Certification” in *SMA 12.4 Administration Guide*.

To enable Central FIPS Licensing:

1. Navigate to **Management Server > Configure > General Settings**.
2. Under **Licensing**, click **Edit**.
3. In the **Online Licensing** section, click **Register**.
4. Log into your MySonicWall account with your username and password.
5. Navigate to **Product Management > My Products**.
6. Expand the line that contains your CMS license.
7. On the **Licenses** page, in the **Gateway Services** section, verify that **FIPS Support** has an active license.

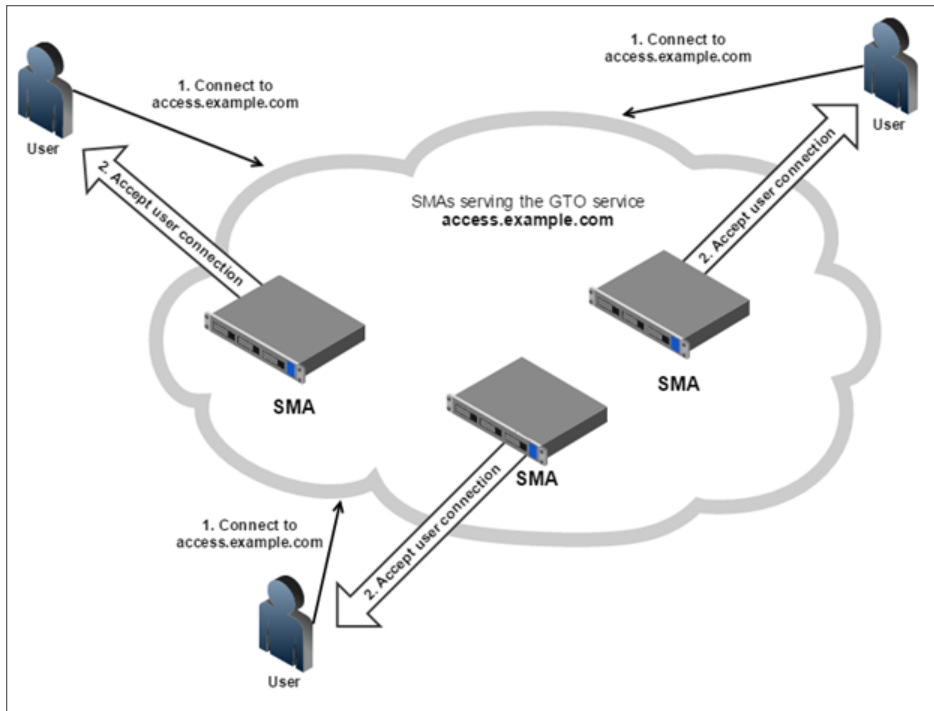
Global High Availability

Topics:

- [Introduction to Global HA and GTO](#)
- [Planning GTO Deployment](#)
- [Setting up GTO](#)
- [Extending GTO Deployment](#)

Introduction to Global HA and GTO

Global High Availability (Global HA) is a set of SMA features that come together to deliver a highly available VPN service. Global HA presents a collection of SMA appliances to end users through a single service name (for example access.example.com). Global Traffic Optimizer (GTO) is the underlying service that is enabled from the CMS console.



Previously, the benefits provided by GTO could only be achieved by deploying and coordinating an array of separate third-party appliances and services, such as content-distribution-network DNS redirectors, local traffic managers, and load balancers often under separate administrative control. GTO replaces this scenario with a single external DNS delegation, which manages all aspects of user traffic distribution automatically, including license provisioning and leveling.

① | **NOTE:** Remember to keep the DNS port open on the firewall.

Users has consistent sign-on procedure with multiple GTO services name that connects them with the appropriate SMA appliance for their current location and circumstances, and gives them a similar experience every time they use the system anywhere in the world.

GTO makes intelligent routing decisions based on real-time data such as appliance availability, health, load, and geographic location. For example, it will be limit the availability of appliances with heavy utilization in order to optimize the performance of your entire GTO environment. GTO directs user connection requests to an available appliance.

This guide provides instructions on how to deploy CMS with GTO, including DNS configuration and certificate requirements.

① | **NOTE:** Administrators can now better see and understand how GTO selects which appliances are chosen to manage user connections. The DNS TXT annotations will have all the information includes A records, NS records, descriptive text, and SOA records.

① | **NOTE:** The TXT interpreter tool can be invoked by running the following query in any GTO enabled appliance as well as CMS `gtdnstxt --name gto_service_name`.

CMS with GTO

CMS with GTO supports the following services and features:

- Exchange ActiveSync and Outlook Anywhere
- Custom FQDN for access to resources and Workplace sites
- Administration visibility into GTO status from the CMS console
- IPv6

Exchange ActiveSync and Outlook Anywhere

From the CMS console, you can configure Exchange ActiveSync and Outlook Anywhere across all appliances in the GTO service. For example, if the GTO service name is **access.example.com** the custom FQDN could be **mail.example.com**.

Mail clients using Exchange ActiveSync or Outlook Anywhere protocol can connect to the GTO service, using a custom FQDN, and experience global traffic Optimizer, such connection to a proximate appliance, improved availability, and load distribution.

① **NOTE:** Public DNS must be configured for the ActiveSync and Outlook Anywhere FQDN, and the names must similar to the GTO service names.

CMS with GTO supports roaming as follows:

- When an Exchange ActiveSync client connects to a GTO service it may get directed to a different appliance from the last time it connected.
- Exchange ActiveSync clients send credentials with each request and after they get authenticated, they can access the ActiveSync server.
- A new pooled license is issued for each connection.
- The license is released after the ActiveSync connection is terminated.

Custom FQDN for Mapped Resources

You can configure custom FQDNs to backend resources across all appliances in a GTO service, and you can access those resources through the appliances that are part of the GTO service.

Users connecting to custom FQDNs can experience the benefits of GTO:

- GTO connection to a proximate appliance
- Improved availability
- Load distribution

Resources should be accessed with the FQDN name rather than with the IP address.

The public DNS must be configured appropriately for each custom FQDN, in that each custom FQDN name must be similar to the GTO service name. For example, if the GTO service name is **access.example.com**, the custom FQDN name for Email should be **mail.example.com**.

The maximum number of custom FQDNs that can be configured for all appliances is the same as that of a standalone SMA appliance. If you are already authenticated to a GTO service, you will need to re-authenticate if you enter a custom FQDN into a Web browser.

You can deploy configurations with the following types custom FQDNs to appliances that are configured for GTO:

- Custom FQDNs that are currently supported on a single appliance.
- Custom FQDN Mapped Resource Access where the backend resource or server is mapped to an external fully qualified domain name (host and domain).
- Workplace site with a domain name that is different from the GTO service domain name.

Viewing GTO Status from the CMS Console

You can view and monitor the following capabilities on the CMC dashboard:

- Appliances successfully enabled for GTO
- Appliances not functioning correctly with GTO
- Appliances that have the recommended certificate SANs for the primary GTO service
- Appliances that do not have the recommended certificate SANs for the primary GTO service
- DNS status of appliances delegated as authoritative servers

GTO and IPv6

- End users on IPv6-only networks can reach SMA appliances with IPv6 addresses through GTO.
- SMA appliances serving as authoritative DNS servers include IPv6 AAAA records in their responses where appropriate.

Deployment Notes

- You should configure a minimum of two SMA appliances and delegate them in DNS as authoritative servers. This minimizes the likelihood that your users ever lose DNS resolution of the GTO service.
- You must enable UDP 53 on your firewall for all traffic that is sent to CMS-managed appliances that are configured as authoritative servers.

Planning GTO Deployment

This section describes how to make deploying GTO easier by planning and adhering to a few guidelines as described below:

Topics:

- [Choosing a Deployment Model](#)
- [Minimizing Configuration Differences](#)
- [GTO Service Names and DNS Delegations](#)
- [Provisioning Certificates](#)

Choosing a Deployment Model

Before you set up your equipment, you need to choose a deployment model that meets your organization's needs. There are several ways you can set up the network hierarchy of your GTO deployment.

SMA Appliances Located in One Data Center

This model is typically employed by mid-sized organizations with major operations in a single location. All their SMA appliances are located in the organization's primary data center. Users have a single GTO service name (such as `access.example.com`) to access the network.

GTO eliminates the need for a load balancer in the data center for VPN traffic. User connections are automatically directed to an available appliance in the data center. The CMS and SMA appliances are all located in the data center. If any one of the appliances fails, the CMS detects the failure, and GTO automatically redirects the VPN connections to another appliance.

SMA Appliances Geo-Distributed across Multiple Data Centers

This model is typically employed by mid-sized organizations with operations in more than one geographic location, and their SMA appliances are located in different geographic locations. For example, an organization deploys two SMA appliances, located in each data center.

The CMS and one of their SMA appliances is located in a data center. The other SMA appliance is located in another data center and also managed by the CMS. All the employees in each data center use a single service name: `access.example.com`, which directs all connections to an available and proximate appliance.

Mixed Mode

This model is typically employed by larger sized organizations with a global workforce. Their SMA appliances are located in multiple geographic locations, and they may have more than one SMA appliance in the data center. For

example, an organization has six SMA appliances: three in New York City, two in London, and one in Tokyo. Employees globally use the same service name: `access.example.com`.

GTO automatically directs connections from employees in the Americas to the SMA appliances in New York City, connections from employees in Europe to the SMA appliances in London, and connections from employees in Asia to the SMA appliance in Tokyo. GTO eliminates the need for a global traffic manager or load balancer in the data center.

Minimizing Configuration Differences

In a GTO service, users can get directed to different SMA appliances frequently, and users expect the same experience, regardless. You can minimize configuration differences between SMA appliances in a GTO service by observing the following guidelines:

- Maintain the same resource set and access rules on each SMA appliance in the GTO service. The best way to do this is to define one central policy on the CMS and synchronize it with all the managed SMA appliances.
- Use wildcard certificates for user access. GTO makes all of its SMA appliances available under a variety of names, each of which must match the certificate. It is possible to identify all such names each time the configuration changes and generate certificates without wildcards. It is recommended that you use Lets Encrypt certificates, support for which is integrated into the CMS.

GTO Service Names and DNS Delegations

To establish a GTO service, you must choose a GTO service name and establish DNS delegations.

Choosing a GTO Service Name

The GTO service name is a delegated DNS zone, which means you must control the parent zone and make a delegation from it to one or more SMA appliances under the GTO service.

If your organization controls the `example.com` DNS zone, the `access.example.com` or `vpn.example.com` could be appropriate GTO service names.

Establishing the GTO Service Name Delegations in DNS

A GTO service name delegation is a DNS subzone delegation. It requires NS records that identify the authoritative server names for the subzone, and corresponding glue-A record that provides IP addresses for those authoritative server names.

DNS delegations must be created for the following components on each of the managed appliances:

- Primary GTO service
- Custom FQDN

- Custom Workplace Sites
- Outlook Anywhere
- Active Sync

The authoritative servers themselves are SMA appliances that are part of the GTO service and are identified by their public IP addresses and the NS record names in the following format:

`<DNSname>.ns.<GTOserviceName>`

For example, the following two DNS records in the zone configuration of example.com could establish a delegation for the GTO service and SMA appliance described above:

```
access.example.com. 86400 IN NS node1.ns.access.example.com
```

```
node1.ns.access.example.com. 86400 IN A xxx.xxx.xx.xx
```

In a typical GTO deployment with multiple SMA appliances, it is important to establish at least two such delegations. This ensures that the GTO service remains available if any one of the SMA appliances is brought down for maintenance (or a network outage).

At least one authoritative server (SMA appliance) must be running at any given moment. Otherwise, users will not be able to connect.

Additional authoritative servers can provide redundancy and improved performance for some users. You should limit GTO service delegations to about three. Ideally, they should be geographically distributed.

Provisioning Certificates

You must provision certificates on the GTO-enabled SMA appliances to facilitate the GTO service. Provisioning certificates must be created for the following components on each of the managed appliances:

- Primary GTO service
- Custom FQDN
- Custom Workplace Sites
- Outlook Anywhere
- Active Sync

Certificates, which give connecting users proof of SMA authenticity before they submit credentials, must be configured on each individual SMA appliance. It is recommended to use Lets Encrypt certificates which is integrated into CMS, and it will automatically be copied to each SMA appliance.

The CMS console Dashboard provides convenient links to the management consoles of each SMA appliance, where certificates are uploaded under SSL Settings.

Topics:

- [Let's Encrypt](#)
- [Adding Certificates to SMA Appliances](#)
- [Generating a Certificate Signing Request \(CSR\)](#)
- [Importing SSL Certificates](#)

Let's Encrypt

Let's Encrypt is a certificate authority that is public, free, API-driven, and trusted by browsers/clients. Integrating Let's Encrypt certificate with SMA enhances the security and eases the deployment process. Let's Encrypt certificates are valid for 90 days and are renewed automatically after 60 days.

In addition, integrating Let's Encrypt certificate with SMA helps to obtain the appropriate SSL certificates when configuring and deploying CMS with GTO.

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).
- The Let's Encrypt must be generated after registering all the SMA appliances and all the GTO services configuration

Creating a Let's Encrypt certificate in CMS

Prerequisites:

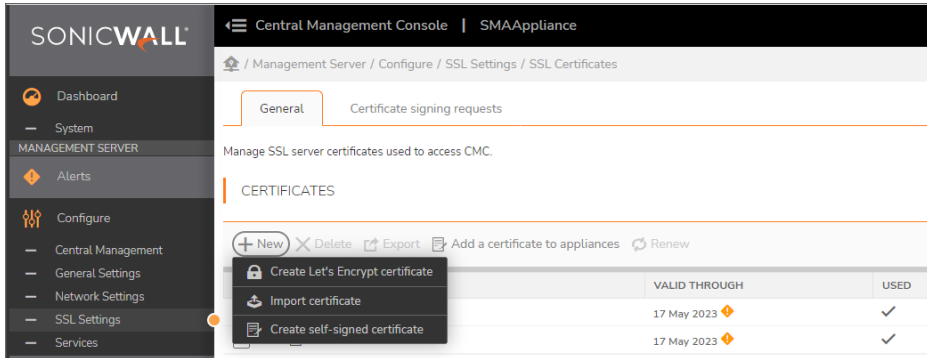
- The CMS must be able to access the Let's Encrypt signing CA over the internet.
- All GTO service names must be delegated in public DNS so that queries are resolved by the GTO authoritative servers.
- The Let's Encrypt signing CA MUST be able to access port 443 on all managed appliances public interface(s) (or via NAT and the appliances must be able to access the CMS on port 443).

To create a Let's Encrypt certificate in CMS:

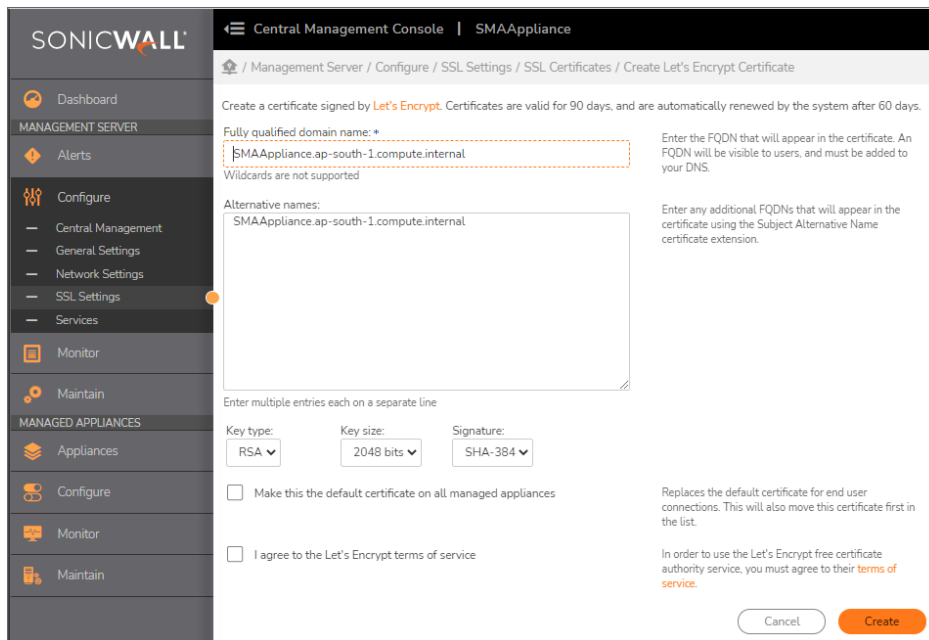
1. Log in to CMS.
2. Navigate to **Management Server > Configure**.
3. Click **SSL Settings**.

The **SSL Settings** page displays,

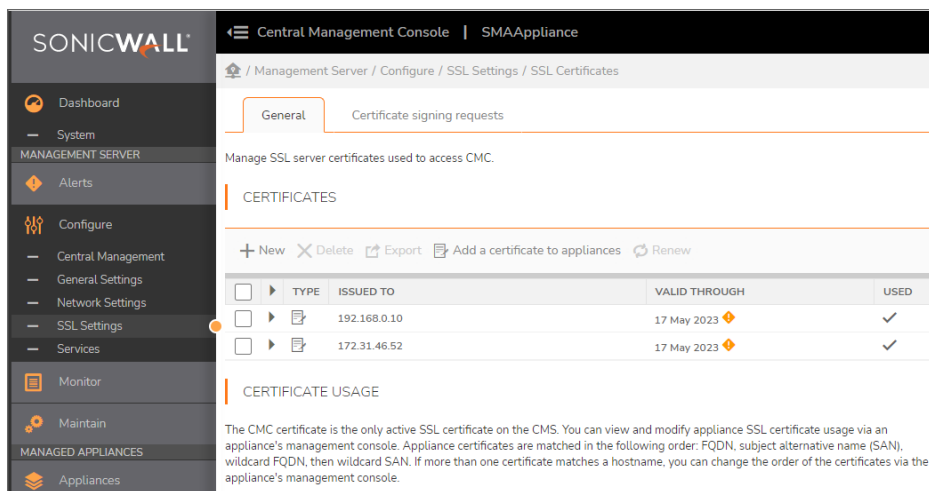
4. Under the **SSL Certificates** group, click **Edit**.
5. In the **General** tab, click **+ New** and select **Create Let's Encrypt certificate** option.



6. In the **Fully qualified domain name** field, enter the complete domain name. The FQDN entered here appears in the certificate and visible to users.
NOTE: Wildcard characters are not supported in the FQDN field.
7. In the **Alternatives names** field, the SAN list is prepopulated for all the required domain names or enter any other name for FQDN. The alternative name entered here appears in the certificate using the SAN certificate extension.
NOTE: Let's Encrypt supports up to 100 SANs per certificate.
8. In the **Key type** drop-down field, select the key type based on your requirement. The supported key types are RSA and EC.
9. 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.
10. 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.
11. 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. If using GTO, this will generate the new Let's Encrypt certificate to all managed appliance and make it as a default certificate in appliances.
12. 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.



The Let's Encrypt certificate is created. You can view and modify the Let's Encrypt certificate.



To view the certificate:

1. Log in to CMS.
2. Navigate to **Management Server > Configure**.
3. Click **SSL Settings**.
The **SSL Settings** page displays,
4. Under the **SSL Certificates** group, click **Edit**.
5. In the **General** tab, under **Certificate Usage** option.

Once you completed creating a Let's Encrypt certificate, browse to the host name and ensure that the certificate is valid and verified

The screenshot shows the SonicWall Central Management Console interface. The left sidebar contains navigation options: Dashboard, Alerts, Configure (with sub-items: Central Management, General Settings, Network Settings, SSL Settings, Services), Monitor, Maintain, and Managed Appliances (with sub-items: Appliances, Configure, Monitor, Maintain). The main content area is titled 'Central Management Console | SMAAppliance' and shows the path 'Management Server / Configure / SSL Settings / SSL Certificates'. The 'General' tab is active, displaying 'Certificate signing requests' and 'Manage SSL server certificates used to access CMC.' Below this is a 'CERTIFICATES' table with columns for TYPE, ISSUED TO, VALID THROUGH, and USED. Two certificates are listed: one issued to 'sonicwallcms1000.com' valid through '16 Aug' and another issued to '192.168.1.1' valid through '17 May'. Below the table is a 'CERTIFICATE USAGE' section with a table mapping hosts to certificates.

HOSTS	CERTIFICATE
Default (WorkPlace/access methods)*	sonicwallcms1000.com
CMC	192.168.1.1
SMAAppliance.ap-south-1.compute.internal (Default)*	sonicwallcms1000.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 screenshot shows a web browser window with the address bar displaying 'https://mc505.eng.sonicwall.com/workplace/access/home'. The page title is 'SONICWALL' and the main content area shows 'Connection Security for mc505.eng.sonicwall.com'. A green lock icon and the text 'You are securely connected to this site.' are visible. A 'Verified by: Let's Encrypt' message is displayed in a white box, with a 'More Information' link below it. The browser's address bar also shows 'Access: Web' and 'Zone: Default zone'.

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:CS: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:B2:8CA3:9F: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

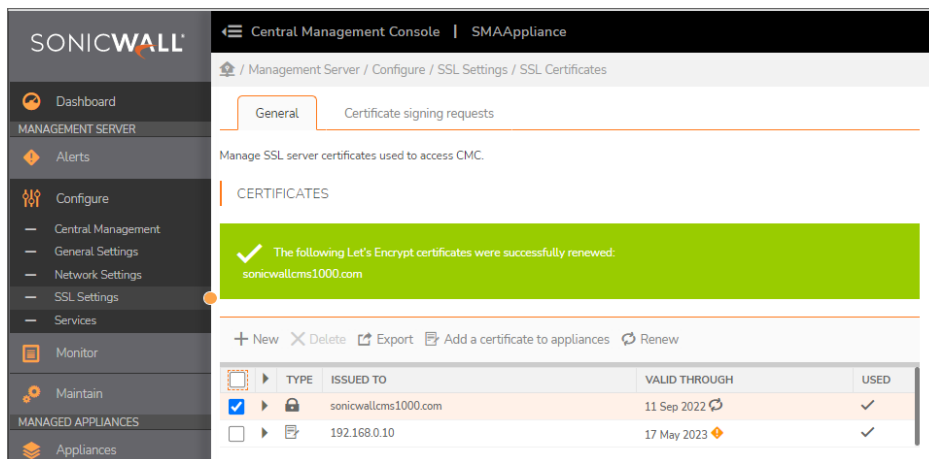
The Let's Encrypt certificates are valid for 90 days and is renewed automatically after 60 days. You can also renew it manually based on your requirements.

To renew the certificate manually:

1. Log in to CMS.
2. In the left panel, select **Management Server > Configure > SSL Settings**.
3. Click **Edit** under the **SSL Certificates** group.

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 displayed under **Valid Through** field.



Adding Certificates to SMA Appliances

To add a certificate to a managed SMA appliance:

1. Add an SSL certificate to the CMS by either:
 - [Generating a Certificate Signing Request \(CSR\)](#)
 - [Importing SSL Certificates](#)
2. Create a maintenance task to add the certificate to the managed SMA appliances. (See [Maintain](#) for more information).

Generating a Certificate Signing Request (CSR)

To generate a certificate signing request:

1. If you want to use wildcard names in the certificate, select **Allow wildcard names**.
 - ① **NOTE:** Using wildcard names can reduce the number of alternative name entries in the certificate. However, it may cost more to get the certificate signed by a Certificate Authority (CA).
2. Select the managed appliances in the table with the missing certificate names.
3. Select the GTO Services names to be included in your certificate request.
4. Click **Generate Certificate Names**.
5. Review the Certificate information to ensure that all expected Subject Alternative Names (SANs) are included in the certificate signing request. Add any missing SANs to the list.
6. Click **Save Certificate Signing Request** to save the CSR.
7. Submit the CSR to a third-party Certificate Authority.
8. When you receive the signed certificate from the Certificate Authority, import the certificate. (See [Importing SSL Certificates](#) for more information).

Importing SSL Certificates

To import an SSL certificate:

1. Navigate to **Management Server > Configure**.
2. Click **SSL Settings**.
3. In the **SSL certificate** section, click **Edit**.
4. In the **Certificates** section, click the **+ New** icon.
5. Select **Import certificate** from the drop-down list.
6. Click **Choose File** to select the certificate file.
7. In the **Password** field, enter the password needed to decrypt the certificate.
8. Click **Import**.

Setting up GTO

This section describes how to configure a basic GTO deployment, consisting of a CMS that manages at two or more SMA appliances.

Topics:

- [Setting up the CMS and SMA appliances](#)
- [Setting up a Basic GTO Service](#)
- [Enabling GTO service for managed appliances with the CMS](#)
- [Monitoring and Configuring GTO](#)
- [Defining the Central Policy](#)

Setting up the CMS and SMA appliances

Before you can configure the GTO, you must first set up a CMS and at least two SMA appliances. GTO uses a distributed data store to share session state and licensing information across the SMA appliances.

① **NOTE:** Managed appliances must be able to communicate with each other via their external interface IP addresses, internal interface IP addresses, or Pool IP addresses in order for them to be able to share information in the distributed data store.

Set up a CMS by following the instructions in [Installing and Configuring the Central Management Server](#) for establishing a CMS virtual machine to control the GTO service and manage the configuration of its component SMA appliances.

Set up the SMA appliances by following the instructions in [Configuring Appliances for Central Management](#). Follow the initial Setup Wizard configuration steps for cabling, administrator password, internal and external interface addresses, routing mode, and gateways, etc.

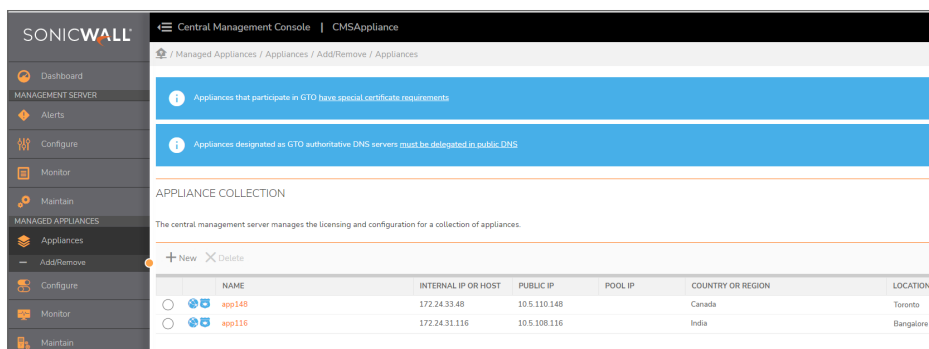
Enabling GTO service for managed appliances with the CMS

① **NOTE:** CMS with GTO supports dual-home (both internal and external interfaces are enabled) or single-home (only the internal interface is enabled) managed appliance.

① **NOTE:** For appliances in the same location, user sessions will increase relative to their user capacity. You must enter the recommended **User Capacity** to avoid the impact of the load score as the user count approaches capacity.

To enable GTO service for managed appliances with the CMS:

1. On the CMS, navigate to **Managed Appliances > Appliances > Add/Remove**.



2. Under **Appliance collection**, click the **+ New** or **Delete** icon to add or modify the managed appliances. For more details on to Add/Remove appliances, see section [Add/Remove](#).

3. Click the appliance name from the CMS list.

NOTE: The client certificate warning, **DNS name** field, and **Public IP** field are only visible when CMS is enabled for GTO.

EDIT APPLIANCE SETTINGS

Display name*: The display name for this appliance

Host name*: The host name for this appliance

Management address*: An appliance IP address or host name that is reachable from the CMS

Public IP*: The appliance IP address that is routable from the Internet, typically this is the appliance external IP address

Public IPv6: The appliance IPv6 address that is routable from the Internet, typically this is the appliance external IPv6 address

Pool IP: The appliance IP address that is reachable by other managed appliances. This is only required if the appliance Public IP is not reachable by other managed appliances.

Country or region: The country or region where this appliance is located

Location: The city, state or province where this appliance is located

Enable Global Traffic Optimizer Service Participate in global high availability services

ma1.cms.sea.eng.sonicwall.com The DNS name for this appliance

This appliance is a public DNS delegation target and must be manually delegated in public DNS

DNS authoritative server This appliance will serve as a DNS authoritative server for all GTO services

Disable this appliance Users connecting to GTO services will not be routed to this appliance. Existing users on this appliance will not be affected. A disabled appliance can serve as a DNS authoritative server.

User capacity: For appliances in the same location, user sessions will increase relative to their user capacity. As the user count approaches capacity, the load score will be affected.

4. In the **Edit Appliance Settings**, select **Enable Global Traffic Optimizer** to participate in Global HA services.
5. Select **DNS authoritative server** to serve as a DNS authoritative server for all GTO services.
6. Select the check box **Disable this appliance** to disable users connecting to GTO service to this appliance. This appliance will remove from the GTO service and will not receive new user connections.

NOTE: Existing user connections will continue on this appliance until the user connections terminates.
7. Modify the **User Capacity**, if the particular appliance needs to handle lower user count than it's default recommended user count.
The User capacity default value depends on the SMA Appliance models:
 - SMA 6200 and 6210- The recommended maximum capacity is 2000 users.
 - SMA 7200 and 7210 - The recommended maximum capacity is 10000 users.
 - SMA 8200v Virtual Appliance- The recommended maximum capacity is 5000 users.
8. Click **Save**.

Setting up a Basic GTO Service

After you set up the Central Management Server (CMS), and at least two SMA appliances, you can set up a basic GTO deployment.

To set up a basic GTO deployment:

1. Navigate to **Management Server > Configure**.
2. Click **Central Management**.
The **Central Management** page displays.

[Home](#) / [Management Server](#) / [Configure](#) / [Central Management](#)

This central management server manages the licensing and configuration for a collection of appliances.

LOCALE

Country or region:

Location:

Example: Seattle, WA

CENTRAL USER LICENSING

Enable central user licensing. The current CMS license will support users and email users across all appliances

GLOBAL TRAFFIC OPTIMIZER SERVICE

Users connect to a global high availability service from anywhere in the world and are routed to an available appliance.

i Each service domain name must be [delegated in public DNS](#)

i Custom GTO services can be created [using central policy resources](#)

[+ New](#) [X Delete](#)

	NAME	DESCRIPTION	DOMAIN	APPLIANCES
No rows to display				

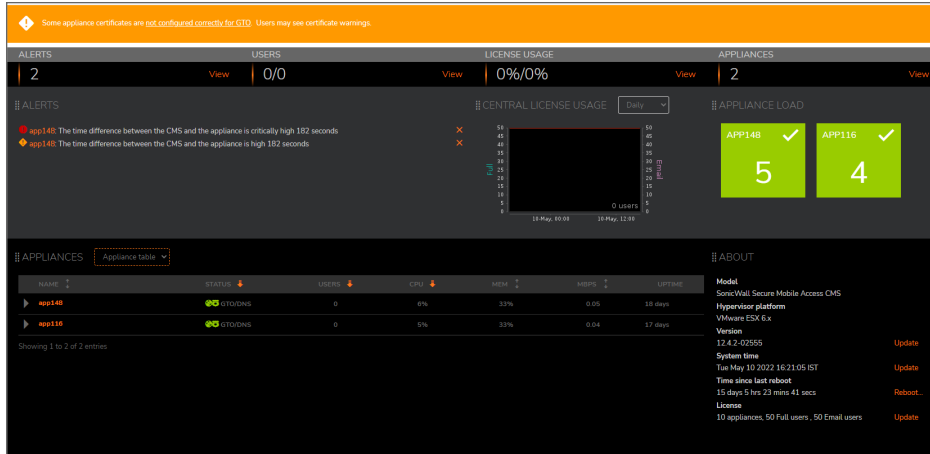
3. Under **Central User Licensing**, select **Enable central user licensing**.
4. Under **Global Traffic Optimizer Service**, select **Users connect to a global high availability service from anywhere in the world and are routed to an available appliance**.

i **NOTE:** The **Global Traffic Optimizer Service** check box is grayed out if **Central User Licensing** is not enabled. You must enable **Central User Licensing** before you enable the **Global Traffic Optimizer Service**.

After you enable the **Global Traffic Optimizer Service**, the following message is displayed:
 The service name must be delegated in public DNS, see the admin guide for details.
5. Under **Global Traffic Optimizer Service**, click **+New** to create a new GTO service, enter the name of your service name. For example, **access.example.com**.
6. Click **Save**.

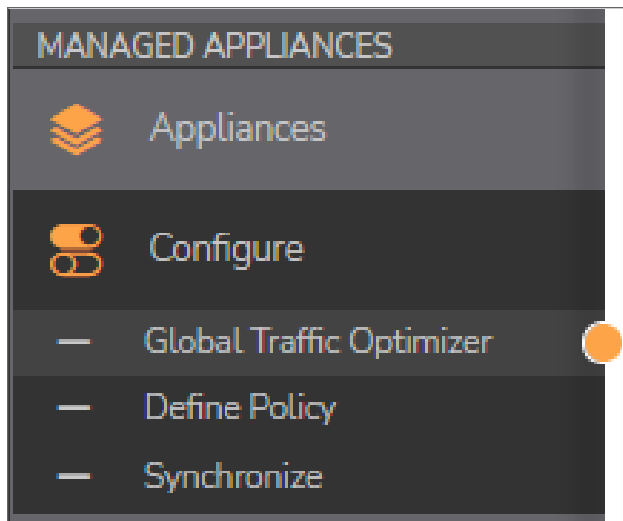
Monitoring and Configuring GTO

The CMC dashboard shows which appliances are participating in GTO. A GTO participant appliance's nominal status is **GTO** with a green globe icon. A non-participant appliance's nominal status is **Managed**. The top of the dashboard displays GTO service warnings and errors, if any.



To manage GTO services:

1. Navigate to **Managed Appliances > Configure**.
2. Click **Global Traffic Optimizer**.



From this page, you can manage the following items:

- Global Traffic Optimizer (GTO)
- Central policies for managed appliances

- Synchronize appliance policies with the central policy

The **GTO Services** page shows a table of all GTO services and their statuses. GTO services are colored green, yellow, or red to reflect their health status. On the lower part of the page is a guide for creating a GTO service with a Custom FQDN, Exchange, or Workplace Site.

Home / Managed Appliances / Configure / Global Traffic Optimizer / GTO Services

GTO Services | Appliance Certificates | DNS Delegations

GTO SERVICES

i Click [here](#) to add managed appliances

i Each service name must be [delegated in public DNS](#)

SERVICE NAME	TYPE	RESOURCE NAME
No rows to display		


CREATE A CUSTOM GTO SERVICE

1. **Enable Policy Synchronization**
2. Define one of the following items in the central policy:
 - URL Resource with Custom FQDN
 - URL Resource with Exchange Server FQDN
 - Realm with a SAML Identity Provider
 - Workplace Site
3. **Synchronize** the central policy with all GTO participant appliances
4. Verify that a new GTO service appears in the table above with a **Service Name** equal to the FQDN of the new resource/site
5. **Follow this guide** to install an supporting certificate on each appliance
6. Verify that the new GTO service appears with a icon in the table above
7. **Follow this guide** to delegate the new GTO service in public DNS
8. Complete! The new GTO service is now accessible to users

The **Appliance Certificates** page shows which Certificate Subject Alternative Names (SANs) must be included in each appliance certificate, and notifies the administrator which SANs are missing.

Home / Managed Appliances / Configure / Global Traffic Optimizer / Appliance Certificates

GTO Services | **Appliance Certificates** | DNS Delegations

 Click [here](#) to enable appliances for the Global Traffic Optimizer Service

ADD AN APPLIANCE CERTIFICATE

Add an SSL certificate to the CMS by [creating a Let's Encrypt certificate](#), completing the CSR process below, or [importing a certificate file](#) then [create a maintenance task](#) to add the certificate to managed appliances

GENERATE A CERTIFICATE SIGNING REQUEST

Generate a Certificate Signing Request containing the required certificate names for the selected appliances and GTO services

Step 1: Choose whether to use wild card names in the certificate
 Step 2: Review **Certificate Status** in the table below and select appliances with missing cert names
 Step 3: Select GTO service names to be included in your certificate request
 Step 4: Review the **Certificate information** to ensure that all expected SANs are included in the CSR
 Step 5: Add any missing SANs to the list
 Step 6: Save CSR
 Step 7: Submit CSR to a third party Certificate Authority for certificate generation
 Step 8: On the [Certificate Signing Requests](#) page process CSR response and import the certificate
 Step 9: [Create a maintenance task](#) to add the certificate to managed appliances

Allow wildcard names This will reduce the number of alternative name entries in the certificate, but may cost more to get signed by a Certificate Authority.


Include Subject Alternative Names for these appliances in the Certificate Signing Request


<input type="checkbox"/>	APPLIANCE NAME	CERTIFICATE STATUS
No rows to display		


The **DNS Delegations** page describes the additional steps an administrator must take to configure the public DNS system for GTO, and provides a helper tool to generate DNS records in BIND format.

Home / Managed Appliances / Configure / Global Traffic Optimizer / DNS Delegations

GTO Services Appliance Certificates **DNS Delegations**

 No appliances are participating in the Global Traffic Optimizer Service. Click [here](#) to enable appliances for the Global Traffic Optimizer Service

 CMS has not been configured to know which appliances are public DNS delegation targets for GTO. Click [here](#) to configure appliances

 GTO services must be configured in public DNS

This page helps you generate the DNS delegation text that you can use to configure public DNS for the GTO services identified in the table below.

Each GTO service name identified in the table must be delegated in public DNS as a subzone delegation.

You must also select SMA appliances that will serve as the DNS authoritative servers for the GTO service names. We recommend that you select at least two SMA appliances from the table below. This ensures that the GTO service remains available if any one of the SMA appliances serving as an authoritative server is brought down for maintenance (or a network outage).

The SMA appliances serving as authoritative servers are identified by their public IP addresses and by NS record names of a specific format:

Hostname.ns.GTOservicename

Each GTO service requires two DNS delegation records for each authoritative server:

- NS record that identifies the authoritative server name for the subzone
- Corresponding "glue-A" record giving the IP address for the authoritative server name

For example, these two DNS records in the zone configuration of **access.example.com** could establish a delegation for GTO service and the SMA appliance **Seattle-01**, which has a Host Name of **seattle01** and a public IP of **172.45.32.11**:

```
access.example.com. 259200 IN NS seattle01.ns.access.example.com.
seattle01.ns.access.example.com. 259200 IN A 172.45.32.11
```

GTO SERVICES

<input type="checkbox"/>	SERVICE NAME	TYPE
No rows to display		

Defining the Central Policy

From the Central Management Console (CMS), you can define the central policy for a single-appliance SMA deployment. You can define the policies for your authentication servers and realms, resources and access rules, web and tunnel access methods, end-point control, and so on. To define the central policy and to synchronize the policy, refer to [Define Policy](#) and [Synchronize](#).

Extending GTO Deployment

Topics:

- [Enabling Cached Credentials](#)
- [Additional Deployment Notes](#)

Enabling Cached Credentials

If your security settings allow cached credentials on end-user devices, you can assign nearly-seamless failover and high-availability capabilities to Connect Tunnel clients and Mobile Connect SSL VPN Tunnel clients. You can do this even if the SMA appliances are in different locations (and therefore do not share an internal network).

To enable cached credentials:

1. Navigate to **Managed Appliances > Configure**.
2. Click **Define Policy**.
3. Click **Realms**.
4. Click on the community for a realm.
5. Click the **Access Methods** tab.
6. In the **Tunnel (IP Protocol)** section, click **Configure**.
7. Scroll down to and expand the **Tunnel Client Options** section.
8. In the **Cached Credentials** section, configure how you want the cached credentials to operate.
For more information on using cached credentials, refer to the *SMA 12.4 Administration Guide*

Additional Deployment Notes

Notes on SMA Appliances

It is recommended that you configure a minimum of two SMA appliances, and that you delegate them in DNS as authoritative servers to minimize the likelihood that your users ever lose DNS resolution of the GTO service.

You must enable UDP 53 on your firewall for all traffic that is sent to CMS-managed appliances that are configured as authoritative servers.

Web Limitations if an Appliance Fails

Web users may face some limitations with GTO if an appliance fails. GTO services should DNS-resolve to more than one MA node, and web browsers given a multi-address DNS response should connect to the first address that works. When CMS finds an MA unresponsive for a minute, it instructs the DNS authoritative server nodes to reconfigure around the broken MA, but during that reconfiguration time, the broken MA node can still appear in DNS responses. If this situation occurs and the user's Workplace session fails, the user sees what looks like a typical failure of a website. The user needs to reconnect by retyping the GTO service name. They are redirected through a different node and can access that web site again.

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 Central Management Server Administration Guide

Updated - January 2024

Software Version - 12.4

232-005699-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/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