



# Secure Mobile Access 12.4

## Common Criteria

### Configuration Guide

SONICWALL®

# Contents

<b>Introduction</b>	<b>4</b>
About This Document	4
Other Related Documents	4
About Secure Mobile Access	5
Target of Evaluation	5
Description	5
Management Interfaces	6
Physical Interfaces	6
Assumptions	7
<b>Common Criteria Configuration</b>	<b>10</b>
Initial access and network configuration	10
Configuring the SMA 8200v	12
Installing the SMA 8200v	12
Powering the SMA 8200v On or Off	14
Configuring Host Settings on the Console	14
Using the Setup Wizard	15
Accessing the Secure Mobile Access Management Console	21
<b>Evaluated Configuration</b>	<b>23</b>
Create a New Local Authentication Server and Configure the Password Policy	24
Create a New Local Administrator	26
Configure Administrator Account User Name and Password Restrictions and Lockout	29
Configure Idle Timeout	31
Configure the Login Banner	33
Disable Services Not Required for the Evaluated Configuration	34
Enable FIPS mode	34
Configure Trusted Certificate Authorities	35
Configure the SMA Web Server Certificate	37
Configure TLS Settings	39
Configure Audit Policy	41
Configure External Audit Server (Syslog)	42
Certificate Requirements	43
Troubleshooting	45
Configure TLS Mutual Authentication	45
Set Other Useful Web Security Options	49

Forcing the use of the HTTPS Protocol .....	49
Preventing the Display of Embedded Web Content .....	51
<b>Auditable Events .....</b>	<b>54</b>
<b>Configuring TLS Certificates on the Client .....</b>	<b>60</b>
<b>Client Certificate Validation .....</b>	<b>61</b>
<b>Certificate Types .....</b>	<b>62</b>
<b>About This Document .....</b>	<b>63</b>

# Introduction

## Topics:

- [About This Document](#)
- [Other Related Documents](#)
- [About Secure Mobile Access](#)
- [Assumptions](#)

## About This Document

This configuration guide provides the information needed to set up SonicWall Secure Mobile Access version 12.4 in the Common Criteria-evaluated configuration that is Network Device collaborative Protection Profile (NDcPP) v2.1 conformant. This guide also includes additional information mandated by the Supporting Document for Network Devices v2.1. Information contained in this document is designed to supplement these documents:

- *SonicWall Secure Mobile Access 12.4 Administration Guide*
- *SonicWall Secure Mobile Access 6210/7210 Getting Started Guide*
- *SonicWall Secure Mobile Access 8200v Getting Started Guide*

## Other Related Documents

### OTHER RELATED DOCUMENTS

Item	Identifier	Short Form
Security Target	SonicWall SMA v12.4 Security Target v0.x	ST
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e, 27 March 2020 (NDcPP)	NDcPP
Administration Guide	<i>SonicWall Secure Mobile Access 12.4 Administration Guide</i>	ADMIN
Getting Started Guide	<i>SonicWall Secure Mobile Access 6210/7210 Getting Started Guide</i>	START
Getting Started Guide	<i>SonicWall Secure Mobile Access 8200v Getting Started Guide</i>	START

# About Secure Mobile Access

## Topics:

- [Target of Evaluation](#)
- [Description](#)
- [Management Interfaces](#)
- [Physical Interfaces](#)

## Target of Evaluation

**Developer:** SonicWall

**Identification:** SonicWall Secure Mobile Access (SMA) 12.4

### PLATFORMS AND DEVICES

Series	Platforms	Build
SonicWall Secure Mobile Access	• SMA 6210	12.4.1-02451
	• SMA 7210	
	• SMA 8200v	

**Claimed Protection Profile:** collaborative Protection Profile for Network Devices v2.2e.

## Description

The SonicWall Secure Mobile Access (SMA) 12.4 in the evaluated configuration consists of these appliances:

- SMA 6210
- SMA 7210
- SMA 8200v

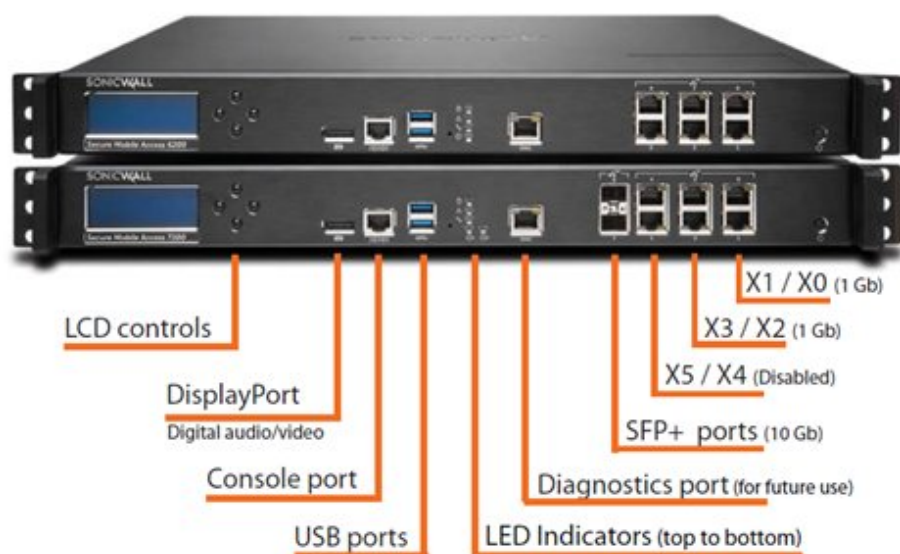
SMA is an access gateway that enables an organization to provide anytime, anywhere and any device access to any internal application. It consists of a hardware appliance with embedded software components. All SMA appliances are shipped ready for immediate access through a Command Line Interface (CLI) and after basic network configuration through a web-based Appliance Management Console (AMC).

# Management Interfaces

The TOE is configured and managed via a web-based Appliance Management Console (AMC) or a local Command Line Interface (CLI). The CLI is accessible from a directly- connected terminal while AMC is accessed remotely via a web browser.

To access the AMC login page after the initial network configuration, point your browser to `https://<IP address>:8443`, where `<IP address>` matches the address you defined for the internal network interface. The default internal network interface IP address is `192.168.0.10`.

## Physical Interfaces



# Assumptions

## ASSUMPTIONS

Assumption Name	Assumption Definition
<b>A.PHYSICAL_PROTECTION</b>	<p>The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.</p>
<b>A.LIMITED_FUNCTIONALITY</b>	<p>The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general-purpose applications (unrelated to networking functionality).</p> <p>In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.</p>
<b>A.NO_THRU_TRAFFIC_PROTECTION</b>	<p>A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on, or is destined to, the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).</p>

Assumption Name	Assumption Definition
<b>A.TRUSTED_ADMINISTRATOR</b>	<p>The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure that passwords or credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
<b>A.REGULAR_UPDATES</b>	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
<b>A.ADMIN_CREDENTIALS_SECURE</b>	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
<b>A.RESIDUAL_INFORMATION</b>	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords, etc.) on the networking equipment when the equipment is discarded or removed from its operational environment.
<b>A.VS_TRUSTED_ADMINISTRATOR</b>	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
<b>A.VS_REGULAR_UPDATES</b>	The VS software is assumed to be updated by an VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities



Assumption Name	Assumption Definition
<b>A.VS_ISOLATION</b>	For vNDs, it is assumed that the VS provides, and is configured to provide, sufficient isolation between software running in VMs on the same physical platform. It is also assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
<b>A.VS_CORRECT_CONFIGURATION</b>	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

# Common Criteria Configuration

## Topics:

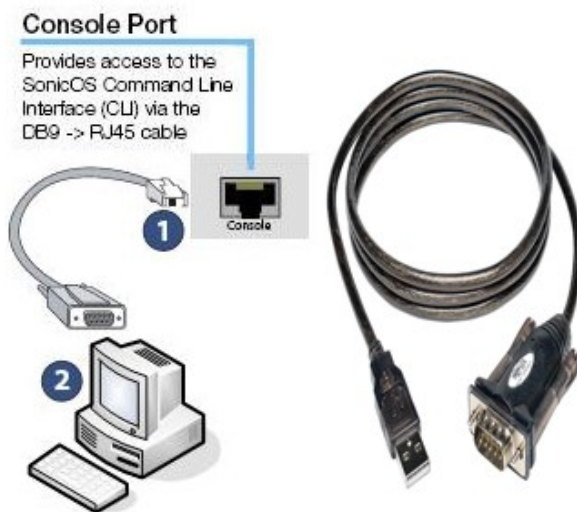
- Initial access and network configuration
- Configuring the SMA 8200v
- Using the Setup Wizard
- Accessing the Secure Mobile Access Management Console
- Evaluated Configuration

## Initial access and network configuration

① **NOTE:** Prior to configuration, download and install the evaluated software version as defined in the **Target of Evaluation** section above.

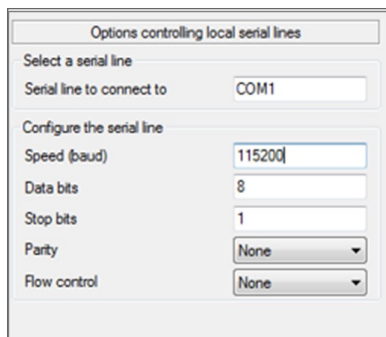
### To configure the network interface:

1. Attach the included null modem cable to the appliance port marked Console Port:



Attach the other end of the null modem cable to a serial port of the management workstation computer.

2. Launch a terminal emulation application that supports serial port communications, such as PuTTY or HyperTerminal.
3. Use these serial line settings:



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

- 115,200 baud
- 8 data bits
- 1 stop bit
- no parity
- no flow control

4. When the serial connection is established, log in to the security appliance for the first time:

```
Welcome User! You are logging into the Management Console
SMAAppliance login: █
```

- a. At the **login:** prompt enter the administrator username.

The default administrator username is `root`.

❶ **IMPORTANT:** Once the Secure Mobile Access appliance has been fully configured, the root account should be disabled.

- b. At the **Password:** prompt, enter the root password.

If an invalid or mismatched username or password are entered, the CLI prompt will return to the **login:** prompt and a CLI administrator login denied due to bad credentials error message will be logged.

5. On initial login, the Secure Mobile Access appliance will initiate an initial configuration prompt:

```
SMAAppliance-c0eae4fda378 login: root
*****
* SonicWall SMA Setup
* Copyright 2016, SonicWall Inc.
*****

Welcome to SonicWall Secure Mobile Access!

The following prompts will guide you through the initial setup of the
SonicWall SMA appliance. The network information you provide here will
enable you to connect to the Administration & Management Console (AMC)
and continue configuring the appliance.

When you're prompted with a question, press "y" for Yes or "n" for No.
To quit, press "q" at any prompt.

[Press any key to proceed] █
```

6. Configure the internal network interfaces:

```
[Press any key to proceed]

INTERNAL INTERFACE CONFIGURATION

Please enter network settings for the internal interface (labeled
"2" on the appliance). If you are on the same network as the appliance,
press ENTER when prompted for a gateway.

IP address: 172.29.0.98
Subnet mask: 255.255.0.0
Gateway: 172.29.0.1
```

7. Once the network interfaces are configured, a conformation message is displayed.

```
Internal network interface configured
IP address: 172.29.0.98
Subnet mask: 255.255.0.0
Gateway: 172.29.0.1

Setup complete!

To continue configuring the appliance, connect to https://172.29.0.98:8443.
See the product documentation for more information.

[Press any key to proceed]
```

8. To terminate the session, enter `logout`.

```
admin@SMAAppliance:~$ logout
```

## Configuring the SMA 8200v

The SMA 8200v can be installed by deploying an OVA file to your ESXi server. Each OVA file contains all related software components needed. Deploy the OVA file by using the vSphere or vCenter client which comes with ESXi. To download the vSphere client, point a browser to your ESXi server and select **Download vSphere Client**.

### Topics:

- [Installing the SMA 8200v](#)
- [Powering the SMA 8200v On or Off](#)
- [Configuring Host Settings on the Console](#)

## Installing the SMA 8200v

### *To install the SMA 8200v using vSphere:*

1. Download the `ex_vm_x.x.x.xxxx.ovf` file from [MySonicWall](#) to a system that is accessible to your ESXi server.  
❗ | **IMPORTANT:** Do not rename the OVA file.

2. Launch vSphere and use it to log on to your ESXi server.
3. In the **Home** screen, navigate to a view that shows the virtual machines running on your ESXi server.
4. To begin the import process:
  - a. Click **File**.
  - b. Select **Deploy OVF Template**.
5. Select **Browse** to locate the OVA file either from a URL to download from or locate it on your system.
6. Click **Next**.
7. Review the details in **OVF Template Details**.
8. Click **Next**.
9. Review the **End User License Agreement**.
10. Click **Accept**.
11. Click **Next**.
12. In the **Name** field, enter a descriptive name for the SMA 8200v appliance.  
The name can contain up to 80 characters and must be unique.
13. From the **Inventory Location** list, select the desired location.
14. Click **Next**.
15. On the **Host / Cluster** page, select the host or cluster on which your virtual appliance is being built.
16. Select **Next**.
17. On the **Resource Pool** page, select the resource pool where you want to deploy the template.
18. Select **Next**.
19. On the **Storage** page, select a destination where you want to store the virtual machine files.
20. Click **Next**.
21. On the **Disk Format** page, review and verify the displayed information.
22. Select the type of provisioning for your disk space.
23. Select **Next**.
24. On the **Network Mapping** pages, select which networks are mapped to this virtual appliance.
25. 23 Select **Next**.
26. On the **Ready to Complete** page:
  - a. Review the options listed.
  - b. Click:
    - **Next** to continue.
    - **Back** to navigate back through the screens to make any changes.
27. Click **Finish** to create your new appliance. The name of the new SMA 8200v appears in the left pane of the vSphere window when complete.

28. The **Deploying** dialog box displays the progress and informs you when the deployment has completed successfully.

## Powering the SMA 8200v On or Off

### *To power the SMA 8200v on or off:*

Use one of these methods to power the SMA 8200v on or off:

- **Method One**
  1. Right-click the SMA 8200v in the left pane.
  2. Navigate to **Power > Power On** or **Power > Power Off**.
- **Method Two**
  1. Select the SMA 8200v in the left pane.
  2. Navigate to the **Getting Started** tab.
  3. Click **Power on the virtual machine** or **Shut down the virtual machine**.
- **Method Three**
  1. Select the SMA 8200v in the left pane.
  2. Navigate to the **Summary** tab.
  3. Click **Power On** or **Shut down guest**.

## Configuring Host Settings on the Console

### *To configure the IP address and default route settings:*

1. Power on the SMA 8200v. (Refer to [Powering the SMA 8200v On or Off](#) for more information.)
2. In vSphere:
  - a. Right-click the SMA 8200v in the left pane.
  - b. Select **Open Console** from the menu.
3. If the virtual machine is not powered on, click the green **Power On** arrow button in the top control bar of the console window.
4. Click inside the window:
  - a. At the login prompt, type **root**.
  - b. Press **Enter**.

The first time you access the console, the **Setup Tool** automatically runs.

① **NOTE:** Your mouse pointer disappears when you click in the console window. To release it, press **Ctrl+Alt**.

5. After the welcome message displays, press any key to proceed.

6. At the **IP address** prompt, enter the local IP address for the SMA 8200v.
7. At the **Subnet** mask prompt, enter the subnet mask.
8. At the **Gateway** prompt, enter the IP address of the default gateway used to access the local interface.
9. Review the information your provided.
10. Press **Enter** to accept these value:
  - **IP address**
  - **Subnet mask**
  - **Gateway**
11. To confirm that you want to save and apply the settings:
  - a. Type **y**.
  - b. Press **Enter**.It may take a few minutes for the initialization process to complete.
12. After the settings are applied, a message is displayed to continue configuration at: `https://<IP address>:8443` (where `<IP address>` is the IP address that you provided).
13. Press **Ctrl+Alt** to activate your cursor.
14. Click the **X** to close the console window.

Setup and basic installation of the SMA 8200v virtual appliance is complete

## Using the Setup Wizard

### *To use the Setup Wizard to configure the SMAappliance:*

1. Access the SMA web management interface using a browser by entering the URL: `https://<IP address>:8443` (where `<IP address>` matches the address configured in the previous section).

① | **NOTE:** The default internal IP address is `192.168.0.10`.

Once connected, you will interact with a Setup Wizard to configure the external interfaces and other configurations for the SMA appliance.

**Welcome**

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

User Access

Completion

### Welcome to SonicWall Secure Mobile Access

This Setup Wizard guides you through a series of required and optional settings for getting the appliance up and running quickly:

- Basic Settings:** Set the password you'll use to administer the appliance, and the date and time.
- Network Settings:** Set the name of the appliance, which is used in log files, and the IP address and subnet mask for the internal and external network interfaces.
- Routing:** Configure the gateways for internal and external network traffic.
- Name Resolution:** Configure the domain name of the network to which the appliance will be connected and the internal DNS.
- User Access:** Create a basic security policy. You can change it later in the Appliance Management Console (AMC).

After you complete the Setup Wizard:

- You will be redirected to AMC. To log in, type "admin" in the Username box, and the enter the administrator password that you set on the Basic Settings page.
- Register your appliance on [MySonicWall](#). Registration gives you access to essential resources, such as your license file and updates. In order to register, you need both the serial number for your appliance, and its authentication code, which is visible on the General Settings page in AMC.

**SONICWALL**  
SECURE MOBILE ACCESS

Cancel < Back Next >

2. Click **Next**.
3. On the **License Agreement** page:

**Welcome**

**License Agreement**

Basic Settings

Network Settings

Routing

Name Resolution

User Access

Completion

### License Agreement

To continue with setup, you must accept the terms of the End User License Agreement. Please read the agreement carefully.

**SonicWall End User Product Agreement**

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO [HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX](https://www.sonicwall.com/legal/eupa.aspx) TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "Agreement") is made between you, the Customer ("Customer" or "You") and the Provider, as defined below.

1. Definitions. Capitalized terms not defined in context shall have the meanings assigned to them below:

Print

☒ I accept the terms of the license agreement

☐ I do not accept the terms of the license agreement

**SONICWALL**  
SECURE MOBILE ACCESS

Cancel < Back Next >

- a. Select **I accept the terms of the license agreement**.
- b. Click **Next**.
4. On the **Basic Settings** page:



- a. In the **Administrator password** fields, enter and confirm the administrator password.
  - b. In the **Date and time** section, from the **Time zone** list, select the time zone associated with the appliance.
  - c. Click **Next**.
5. On the **Network Settings** page, in the **External Interface** section:

- a. In the **IP address** field, enter the external IP address.
  - b. In the **Subnet mask** field, enter for the external subnet mask.
  - c. Click **Next**.
- ① **NOTE:** The values in the **Internal Interface** section will be already filled in based on the values set during the initial configuration using the AMC setup tool.

6. On the **Routing** page:

Welcome

License Agreement

Basic Settings

Network Settings

**Routing**

Name Resolution

User Access

Completion

**Routing**

To leverage an existing router, select the dual gateway option to reach your resources. To restrict incoming appliance traffic to only a few routes or subnets, select a single gateway option and enter the routes or subnets as static routes later in AMC.

If you plan to access AMC from a computer on a different subnet than the appliance (172.16.1.44/255.255.255.0), you must configure an internal 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:  
Dual gateway

Internal gateway IP address:  
172.16.1.1

External gateway IP address:  
172.16.0.1

SONICWALL  
SECURE MOBILE ACCESS

Cancel < Back Next >

- From the **Routing mode** list, select **Dual gateway**.
- In the **Internal gateway IP address** field, the value will already be filled in based on the values set during the initial configuration using the AMC setup tool.
- In the **External gateway IP address** field, enter the IP address of the external gateway.
- Click **Next**.

7. On the **Name Resolution** page:

The screenshot shows the 'Name Resolution' configuration page in the SonicWall Secure Mobile Access interface. On the left is a navigation menu with options: Welcome, License Agreement, Basic Settings, Network Settings, Routing, Name Resolution (highlighted), User Access, and Completion. The main content area is titled 'Name Resolution' and includes a description: 'Specify the domain in which the appliance is located and the primary DNS server used for name resolution. This allows the appliance to reach resources on your internal network by name.' Below this are two fields: 'Default domain: \*' with a text input field and a help text 'The domain in which the appliance is located (such as example.com).', and 'DNS Server:' with a text input field and a help text 'Enter the IP address for your primary DNS server. More DNS servers can be added later in AMC.' At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'.

- In the **Default domain** field, enter the domain in which the appliance is located.
- In the **DNS Server** field, enter the IP address for the primary DNS server.
- Click **Next**.

8. On the **User Access** page:

The screenshot shows the 'User Access' configuration page in the SonicWall Secure Mobile Access interface. The navigation menu on the left is the same as in the previous screenshot, with 'User Access' highlighted. The main content area is titled 'User Access' and includes a section 'Access Methods' with a description: 'The SonicWall Secure Mobile Access appliance provides several different agents for graded levels of access to backend resources. Select this option to provision the OnDemand Tunnel access agent for full network access:'. Below this is a checkbox labeled 'Enable full network access using OnDemand Tunnel'. To the right of the checkbox is a field for 'NAT address for network tunnel traffic: \*' with a text input field and a help text 'The NAT address for network tunnel traffic must be on the same subnet as the internal interface (172.16.1.44/255.255.255.0)'. Below the checkbox is a section 'Access Policy' with a description: 'The SonicWall Secure Mobile Access appliance uses a granular access policy to determine what backend resources a given user is allowed to access. Select an initial access policy for users:'. There are three radio button options: 'Allow authenticated users access to all defined resources' (selected), 'Allow authenticated users access to the entire network', and 'Initially deny all access'. Each option has a brief description of its effect. At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'.

- Enter an IP address for **NAT address for network tunnel traffic** and select an **Access Policy**.
- Click **Next**.

① | **NOTE:** These settings are optional can be configured later.

9. On the **Completion** page, review all of the configured settings.

Welcome
License Agreement
Basic Settings
Network Settings
Routing
Name Resolution
User Access
**Completion**

## Completion

You have successfully completed the Setup Wizard.

To apply your settings, click **Finish**. After your settings have been applied, you will be directed to AMC where you can login using the password you supplied earlier.

**Appliance Settings**

Date and time:	Fri Apr 23 2021 18:49:21 BST
Appliance name:	SMAAppliance
Internal interface:	172.16.1.44 / 255.255.255.0
External interface:	172.16.0.44 / 255.255.255.0
Routing:	Dual gateway (172.16.0.1, 172.16.1.1)
Default domain:	sonicwall.com
DNS server:	Not configured
Full network access:	OnDemand Tunnel disabled
Access policy:	Allow authenticated users access to all defined resources


SONICWALL  
SECURE MOBILE ACCESS

Cancel
< Back
Finish

- Click **Back** to go back and change any of the settings.
- Click **Finish** to apply the changes.

Welcome
License Agreement
Basic Settings
Network Settings
Routing
Name Resolution
User Access
Completion

## Completion

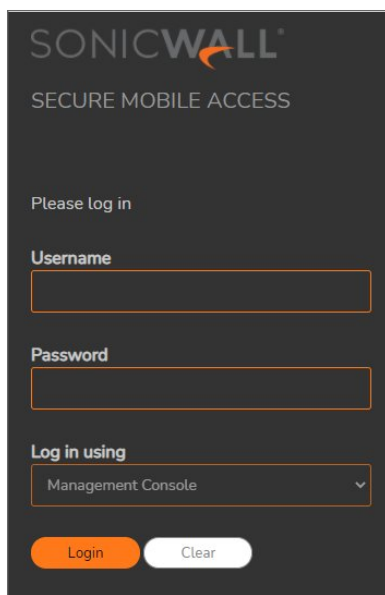
 **Applying changes. Please wait...**

SONICWALL  
SECURE MOBILE ACCESS

# Accessing the Secure Mobile Access Management Console

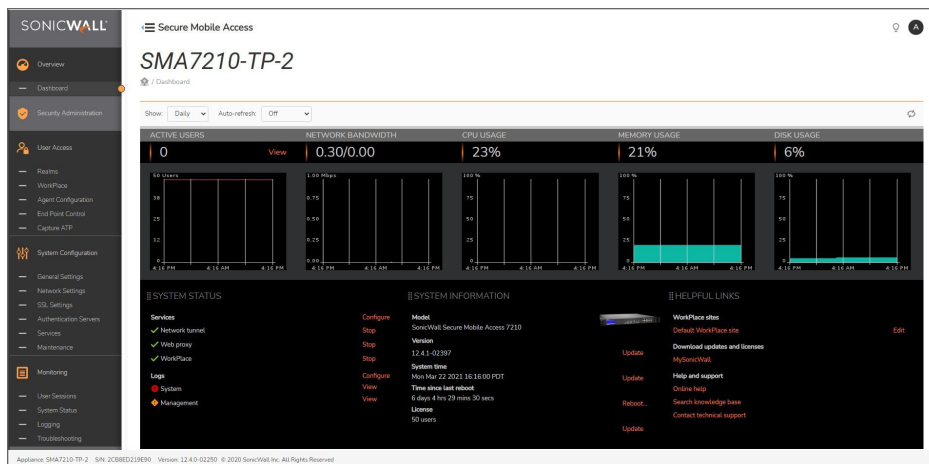
## To access the Secure Mobile Access Management Console (AMC):

1. Using a browser, enter the URL: `https://<IP address>:8443` (where *<IP address>* matches the IP address of the internal network interface.  
① | **NOTE:** The default IP address is `192.168.0.10`.
2. Enter the previously configured credentials to authenticate to the AMC.

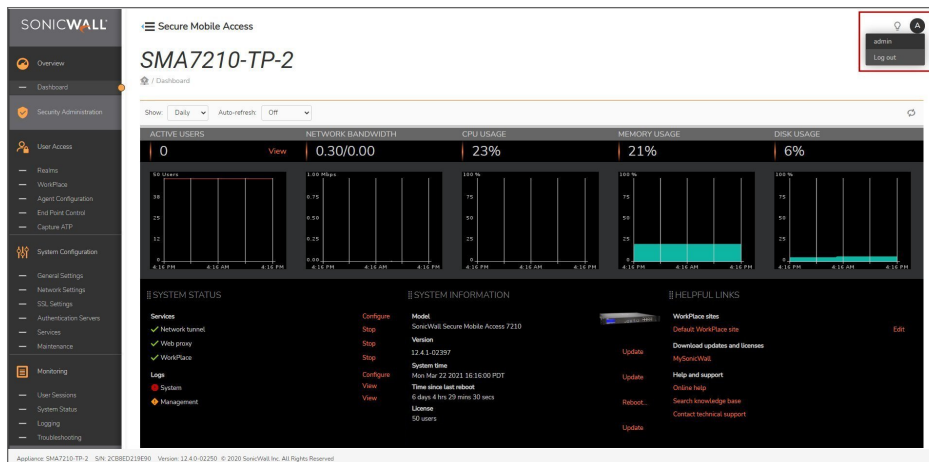


The login page for the SonicWall Secure Mobile Access Management Console (AMC). It features the SonicWall logo at the top, followed by the text "SECURE MOBILE ACCESS". Below this, it says "Please log in". There are two input fields: "Username" and "Password". Below the password field is a "Log in using" dropdown menu with "Management Console" selected. At the bottom are two buttons: "Login" (orange) and "Clear" (white).

3. Once successfully authenticated, the AMC dashboard will be displayed.

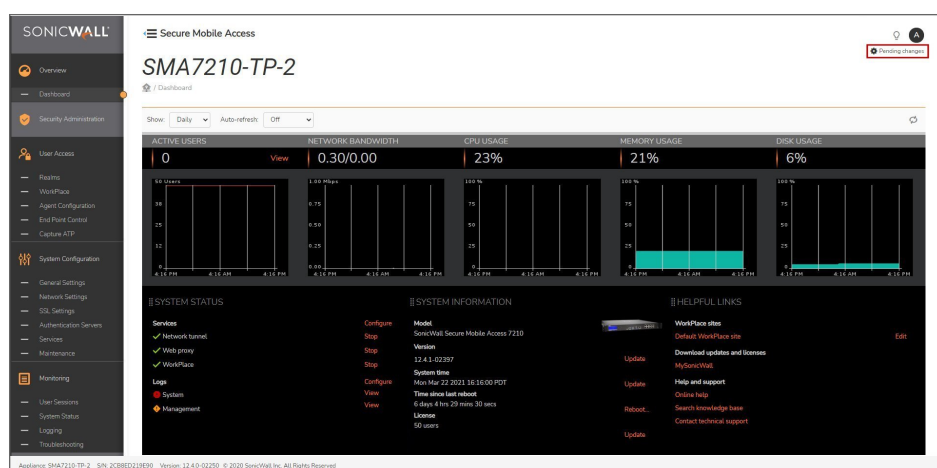


4. To terminate the AMC session, click **Log out** in the top right corner.



# Evaluated Configuration

① | **NOTE:** Some configuration changes require applying pending changes to take effect.



1. Create a New Local Authentication Server and Configure the Password Policy
2. Create a New Local Administrator
3. Configure Administrator Account User Name and Password Restrictions and Lockout
4. Configure Idle Timeout
5. Configure the Login Banner
6. Disable Services Not Required for the Evaluated Configuration
7. Enable FIPS mode
8. Configure Trusted Certificate Authorities
9. Configure the SMA Web Server Certificate
10. Configure TLS Settings
11. Configure Audit Policy
12. Configure External Audit Server (Syslog)

13. [Configure TLS Mutual Authentication](#)
14. [Improve Performance on Isolated Networks](#)

## Create a New Local Authentication Server and Configure the Password Policy

**To create a new local Authentication Server and configure the Password Policy:**

1. Log in to the Appliance Management Console using administrator credentials.
2. Navigate to **System Configuration > Authentication Servers**.
3. In the **Authentication Servers** section, click **New....**
4. In the **User Store** section, under **Local users storage**, select **Local users**. Leave the other settings unchanged.

The screenshot shows the SonicWall Appliance Management Console interface. On the left is a navigation menu with categories like Overview, Security Administration, User Access, System Configuration, Services, Maintenance, and Monitoring. The 'System Configuration' section is expanded, showing 'Authentication Servers' as the current page. The main content area is titled 'Add Authentication Server' and includes a breadcrumb trail: 'Authentication Servers / Add Authentication Server'. Below this, there's a prompt to 'Choose the protocol used to access your user store, and specify how users will authenticate. Click Continue to configure the authentication server.' The 'USER STORE' section asks to 'Choose the directory type or authentication method:' and lists several options under 'Authentication directory' (Microsoft Active Directory (Basic), Microsoft Active Directory (Advanced), LDAP, RADIUS, One Identity Defender, RSA Authentication Manager, Public key infrastructure (PKI), SAML 2.0 Identity Provider) and 'Local user storage' (Local users). The 'Local users' option is selected. The 'CREDENTIAL TYPE' section asks to 'Specify how users will authenticate:' and lists 'Digital certificate', 'Token/SecurID', and 'Username/Password'. The 'Username/Password' option is selected. At the bottom right, there are 'Cancel' and 'Continue' buttons, with 'Continue' being highlighted in orange.

5. Click **Continue....**



6. On the **Edit Authentication Server** page:

**SONICWALL** Secure Mobile Access

## Edit Authentication Server

Authentication Servers / Edit Authentication Server

Configure authentication settings for local users.

**Credential type:** UsernamePassword

Name\*  
local-auth

---

**PASSWORD POLICY**

Passwords are  to  characters in length

Passwords must contain at least one of the following

<input checked="" type="checkbox"/> Lowercase letters	<input checked="" type="checkbox"/> Uppercase letters
<input checked="" type="checkbox"/> Numeric digits (0-9)	<input checked="" type="checkbox"/> Symbols (~`!@#\$%^&*()_+={} \\:;'"<,>./)

---

**PASSWORD EXPIRATION**

☐ Passwords expire after  days

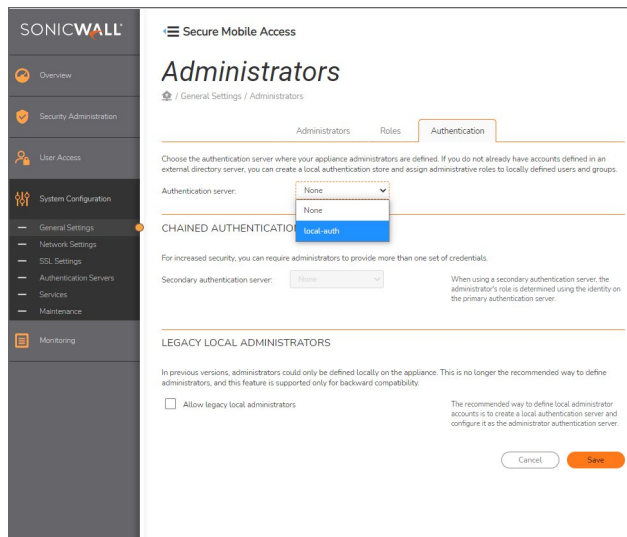
☐ Begin prompting user  day(s) before password expires

> ADVANCED

Cancel Save

- In the **Name** field, enter `local-auth`.
  - In the **Password Policy** section, select all of these options:
    - **Lowercase letters**
    - **Uppercase letters**
    - **Numeric digits (0-9)**
    - **Symbols (~`!@#\$%^&\*()\_+={}|\\:;'"<,>./)**
  - Click **Save**.
- Navigate to **System Configuration > General Settings**.
  - In the **Administrators** section, click **Edit**.
  - Click **Authentication**.

10. From the **Authentication server** list, select **local-auth**.



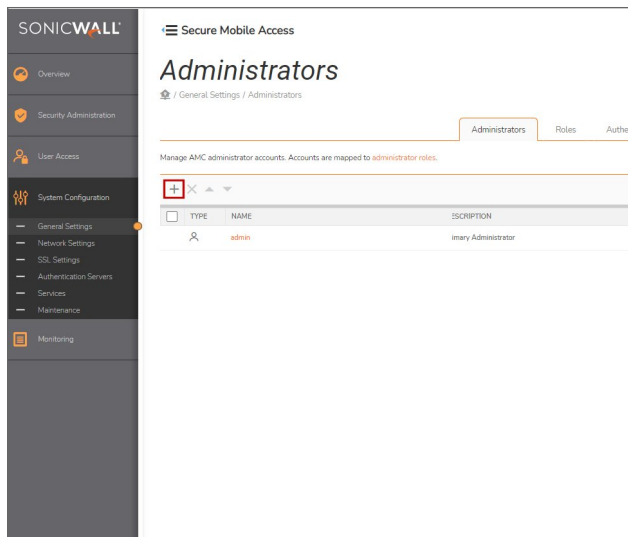
11. Click **Save**.
12. Click **Pending Changes** to apply these configuration changes.

## Create a New Local Administrator

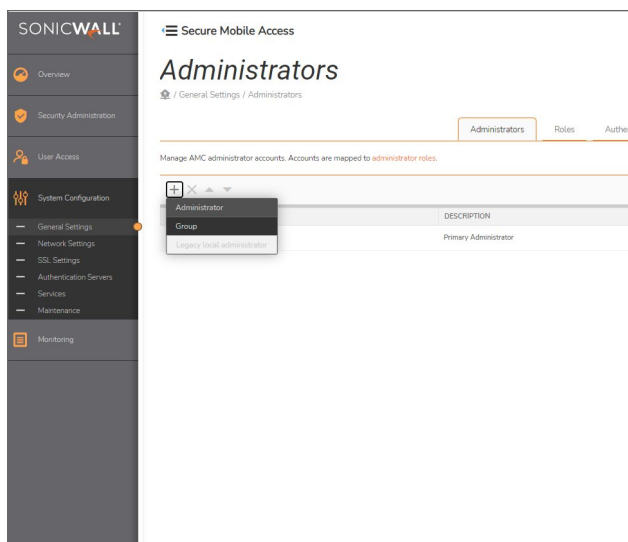
### *To create a new local administrator:*

1. Navigate to **System Configuration > General Settings**.
2. In the **Administrators** section, click **Edit**.
3. Click **Administrators**.

4. Click the New (+) icon.



5. From the list, select **Administrator**.



6. On the **Add Administrator** page:
- From the **User** list, select the user account you want to assign as the local administrator.
  - From the **Role** list, select the type of administrator for the new local administrator.
  - Click **Save**.

**SONICWALL** Secure Mobile Access

## Add Administrator

[Home](#) / [General Settings](#) / [Administrators](#) / [Add Administrator](#)

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

User:

Role:

The new local administrator account is displayed in the **Administrators** list.

**SONICWALL** Secure Mobile Access

## Administrators

[Home](#) / [General Settings](#) / [Administrators](#)

[Administrators](#) [Roles](#) [Authn](#)

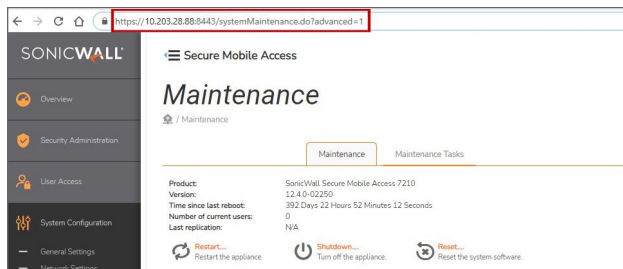
Manage ABC administrator accounts. Accounts are mapped to administrator roles.

TYPE	NAME	DESCRIPTION
<input type="checkbox"/>	admin	Imaginary Administrator
<input type="checkbox"/>	cc-admin	

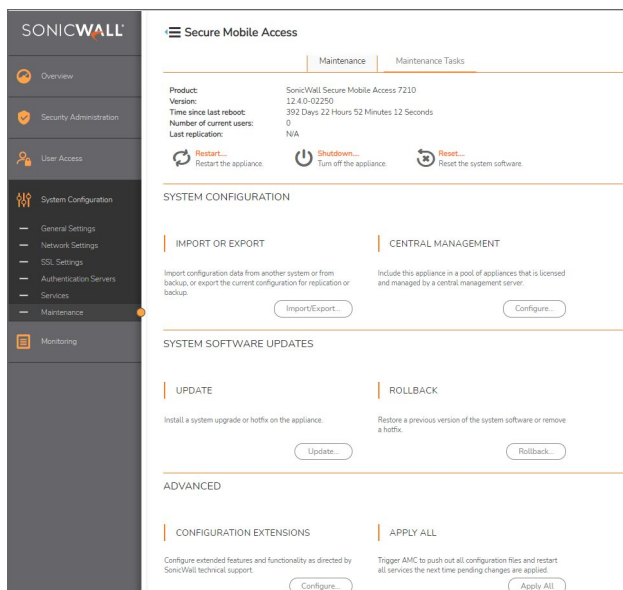
# Configure Administrator Account User Name and Password Restrictions and Lockout

*To configure an administrator account user name and password restrictions and lockout:*

1. Navigate to **System Configuration > Maintenance**.
2. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.

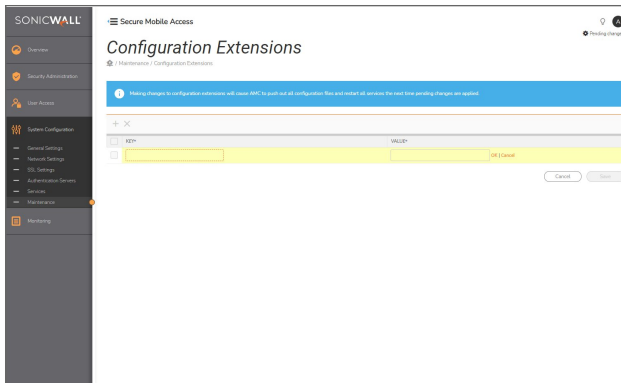


3. Scroll down to the **Advanced > Configuration Extensions** section.



4. Click **Configure....**

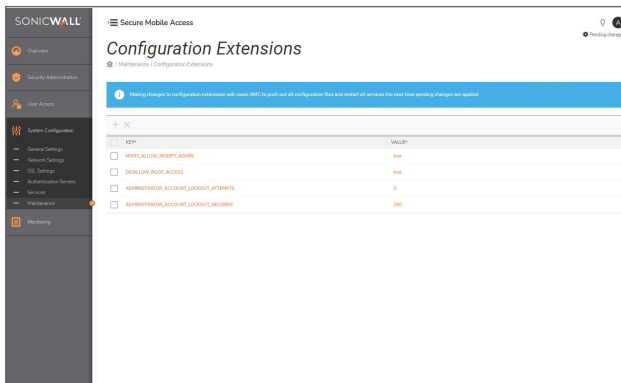
- On the **Configuration Extensions** page, click the New (+) icon.



- In the table:

- For the **Key** enter `MGMT_ALLOW_MODIFY_ADMIN`, for the **Value** enter `true`, and click **OK**.
- For the **Key**: `DISALLOW_ROOT_ACCESS`, for the **Value** enter `true`, and click **OK**.
 

**NOTE:** When root access is disabled, only Primary Administrators can access the command-line interface (CLI).
- For the **Key**: `ADMINISTRATOR_ACCOUNT_LOCKOUT_ATTEMPTS`, for the **Value** enter the threshold (the number of successive unsuccessful authentication attempts) (3), and click **OK**.
- For the **Key**: `ADMINISTRATOR_ACCOUNT_LOCKOUT_SECONDS`, for the **Value** enter the lockout period in seconds (180), and click **OK**.



- Click **Save**.
- Navigate to **Security Administration > Users & Groups**.
- Click **Local Accounts**.
- Click the name of the account you want to rename.

11. On the **Edit Local User** page, in the **Username** field, enter a custom user name.

The screenshot shows the 'Edit Local User' page in the SonicWall management interface. The left sidebar contains navigation options: Overview, Security Administration, User Access, System Configuration, and Monitoring. The main content area is titled 'Edit Local User' and includes a breadcrumb trail 'Users & Groups / Edit Local User'. Below the title, there is a section 'Create a user in a local directory.' with input fields for 'Username' (containing 'cc-admin') and 'Description'. To the right of these fields is a placeholder text 'Type a username for a local user.' Below the 'Username' field is a 'Password' field and a 'Confirm password' field, with a placeholder text 'Type a password for the local user.' to the right. There are three checkboxes: 'User is enabled' (checked), 'Reset password for this user' (unchecked), and 'User must change password at next login' (unchecked). At the bottom right, there are 'Cancel' and 'Save' buttons.

12. Click **Save**.

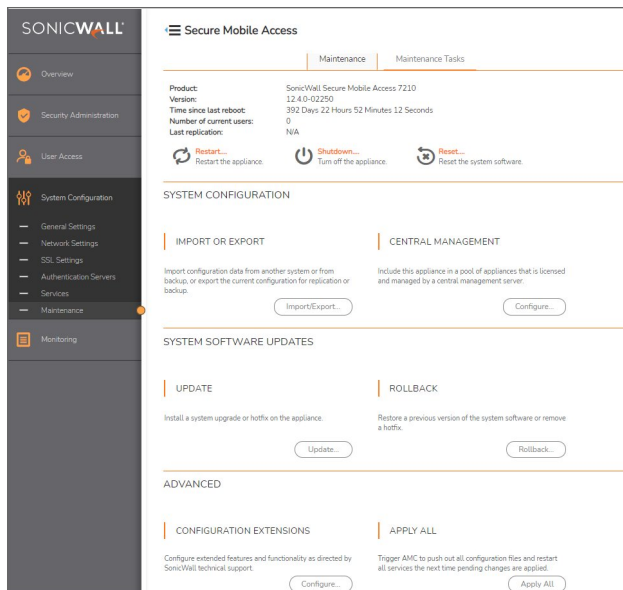
## Configure Idle Timeout

*To configure the idle timeout:*

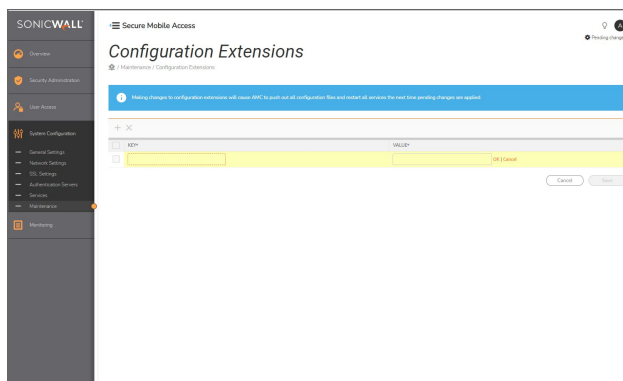
1. Navigate to **System Configuration > Maintenance**.
2. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.

The screenshot shows the 'Maintenance' page in the SonicWall management interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Maintenance' and includes a breadcrumb trail 'Maintenance'. Below the title, there is a section 'Maintenance' with a sub-section 'Maintenance Tasks'. The 'Maintenance' section displays system information: Product (SonicWall Secure Mobile Access 7210), Version (12.4.0-02250), Time since last reboot (392 Days 22 Hours 52 Minutes 12 Seconds), Number of current users (0), and Last replication (N/A). Below this information are three buttons: 'Restart' (Restart the appliance), 'Shutdown' (Turn off the appliance), and 'Reset' (Reset the system software).

3. Scroll down to the **Advanced > Configuration Extensions** section.

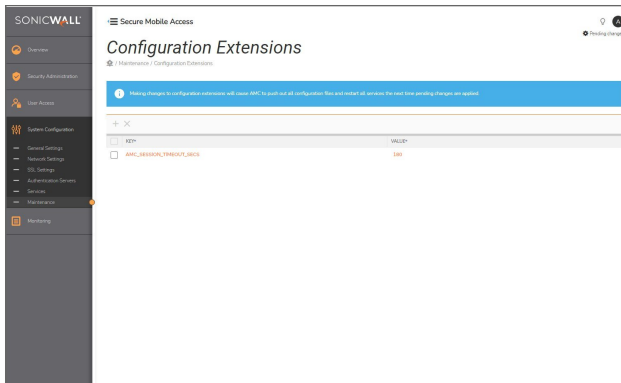


4. Click **Configure...**.
5. On the **Configuration Extensions** page, click the New (+) icon.



6. In the table:
  - For the **Key** enter `AMC_SESSION_TIMEOUT_SECS`, for the **Value** enter idle timeout in seconds (180), and click **OK**.



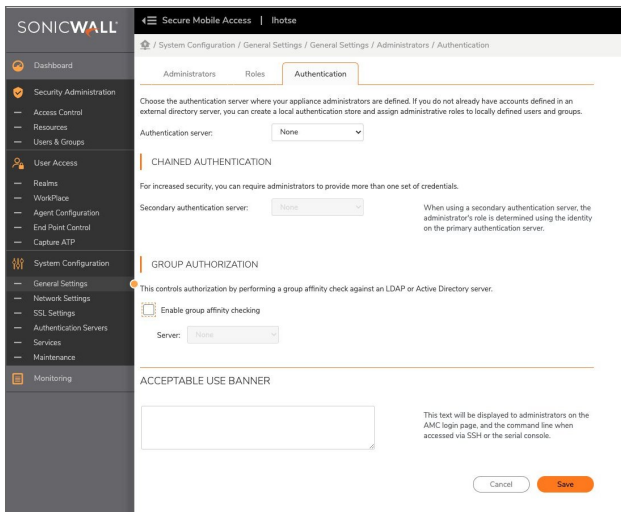


7. Click **Save**.
8. Click **Pending Changes** to apply these configuration changes.

## Configure the Login Banner

*To configure the login banner:*

1. Navigate to **System Configuration > General Settings > Administrators > Authentication**.



2. In the **Acceptable Use Banner** section, enter the content you want displayed when an administrator logs in to the appliance.
3. Click **Save**.
4. Click **Pending Changes** to apply these configuration changes.

# Disable Services Not Required for the Evaluated Configuration

## To check the status of services:

1. Navigate to **System Configuration > Services**.
2. Verify that these services are disabled:
  - **SNMP**
  - **SMTP**
  - **SSH**

NETWORK SERVICES	
<b>NTP</b> Synchronize the system clock with an external Network Time Protocol (NTP) server. <a href="#">Configure</a>	Status: <b>Disabled</b>
<b>SSH</b> Use Secure Shell (SSH) to safely access the appliance command line from another host. <a href="#">Configure</a>	Status: <b>Disabled</b>
<b>SNMP</b> Monitor the appliance from a Simple Network Management Protocol (SNMP) management tool. <a href="#">Configure</a>	Status: <b>Disabled</b>
<b>SMTP</b> Allow the system to send email using a Simple Mail Transfer Protocol (SMTP) mail server. <a href="#">Configure</a>	Status: <b>Disabled</b>
<b>SMS</b> Allow the system to send text messages using a Short Message Service (SMS) provider. <a href="#">Configure</a>	Status: <b>Disabled</b>

## To disable a service:

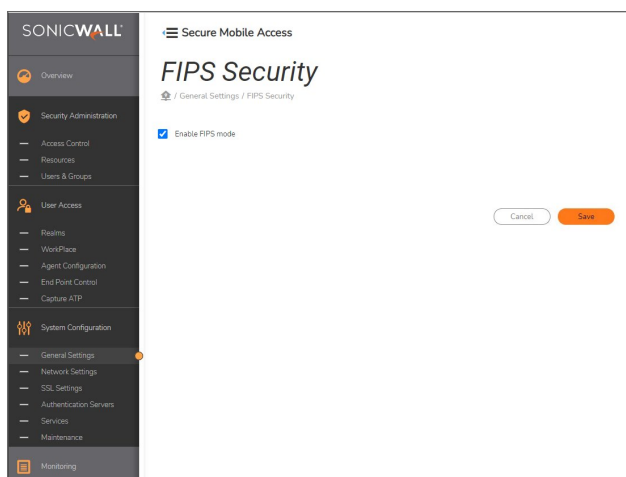
1. Navigate to **System Configuration > Services**.
2. For each service you want to disable:
  - a. Click **Configure**.
  - b. Select **Disable <service name>**.
3. Click **Save**.
4. The status for the service should display as **Disabled**.

# Enable FIPS mode

⚠ **CAUTION:** Enabling FIPS mode will delete any existing keys and certificates.

### To enable FIPS mode:

1. Navigate to **System Configuration > General Settings**.
2. In the **FIPS Security** section, next to **FIPS Security**, click **Edit**.
3. Click **Enable FIPS mode**.



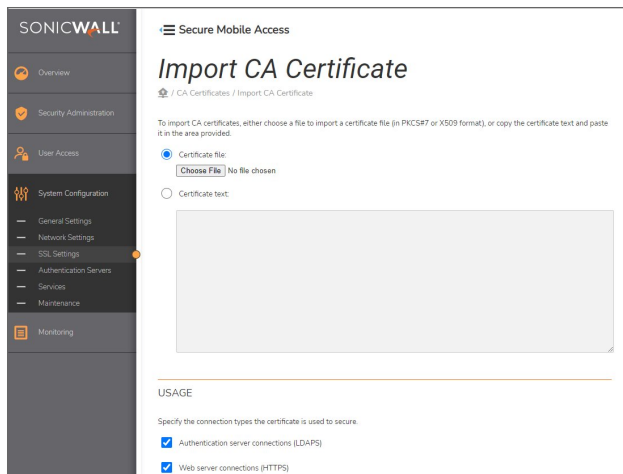
4. Click **Save**.
5. Click **Pending Changes** to apply these configuration changes, and wait for the appliance to restart

## Configure Trusted Certificate Authorities

① **NOTE:** If OCSP signing is delegated to a different certificate authority (CA), those CA certificates also must be explicitly trusted and configured as a designated responder.

### To configure trusted certificates:

1. Navigate to **System Configuration > SSL Settings**.
2. Next to **CA Certificates**, click **Edit**.
3. Click the New (+) icon.
4. On the **Import CA Certificate** page, select **Certificate file** and click **Browse**.



5. In the **Usage** section, select:

- **Web Server connections (HTTPS)**
- **OCSP response verification**

① | **NOTE:** Other **Usage** settings may be applicable, depending on your specific deployment scenario.

6. Click **Import**.

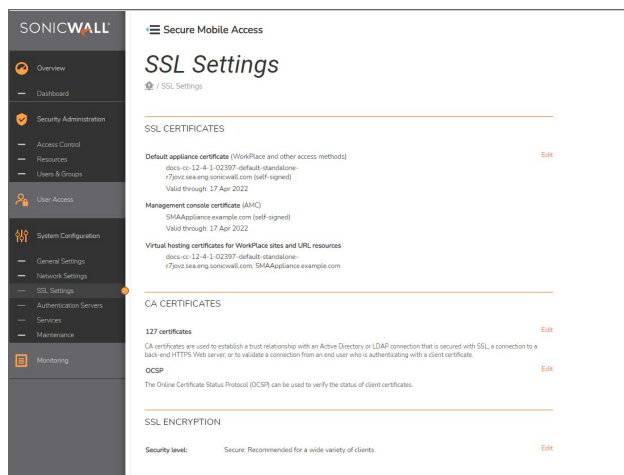
① | **NOTE:** SMA comes preloaded with a set of public Certificate Authorities. Review and remove them according to your organizational policies. Any certificates issued by any CA on this list would be trusted by SMA.

# Configure the SMA Web Server Certificate

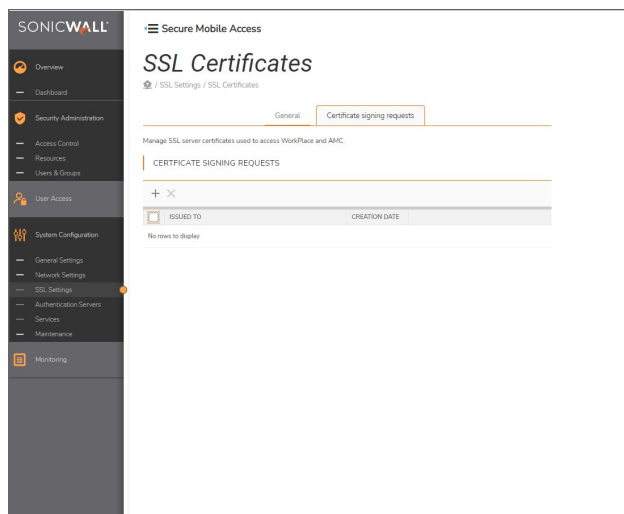
① **NOTE:** The SMA web certificate must be signed by a trusted Certificate Authority and must not be expired or revoked at the time of loading.

*To configure a SMA web server certificate:*

1. Navigate to **System Configuration > SSL Settings**.
2. Next to **SSL Certificates**, click **Edit**.



3. On the **SSL Certificates** page, click **Certificate Signing Requests**.



4. Click the New (+) icon.

5. In the **Certificate Information** section enter the required information in the fields.
- ❗ | **IMPORTANT:** Verify that Alternative names field that corresponds to SAN extension contains a unique identifier in form of FQDN or IPv4 address.

The screenshot shows the SonicWall Secure Mobile Access interface. The left sidebar contains navigation links: Overview, Dashboard, Security Administration, Access Control, Resources, Users & Groups, User Access, System Configuration (highlighted), General Settings, Network Settings, SSL Settings (highlighted with an orange dot), Authentication Servers, Services, and Maintenance. The main content area is titled 'Create Certificate Signing Request' and includes a breadcrumb trail: 'SSL Settings / SSL Settings / Create Certificate Signing Request'. Below the title, it says 'Create a CSR for use in obtaining an SSL certificate from a commercial CA.' The 'CERTIFICATE INFORMATION' section contains the following fields and instructions:

- Fully qualified domain name:** This name will appear in the certificate. It will be visible to users, and must be added to your DNS.
- Alternative names:** Enter any additional FQDNs (or IP addresses) that will appear in the certificate using the Subject Alternative Name certificate extension. (Note: Enter multiple entries each on a separate line.)
- Organizational unit:** Your division or department. For example, HR Dept.
- Organization:** For example, ABC Corporation. Most commercial CAs require you to enter this exactly as it appears on your articles of incorporation.
- Locality:** For example, Seattle. No abbreviations.
- State:** No abbreviations.
- Country:** Two-letter abbreviation only for example US or AU.

At the bottom, there are three dropdown menus: **Key type:** RSA, **Key size:** 2048 bits, and **Signature:** SHA-384.

6. From the **Key type** list, select the key type. This can be either **RSA** or **EC** (elliptic curve). The default value is **RSA**.

- When generating an RSA key:

1. From the **Key size** list, select the key length you want to use for the key:

1. **2048 bits** (default)
2. **3072 bits**
3. **4096 bits**

❗ | **NOTE:** Larger keys increase security.

2. From the **Signature** list, select the algorithm used for the certificate.

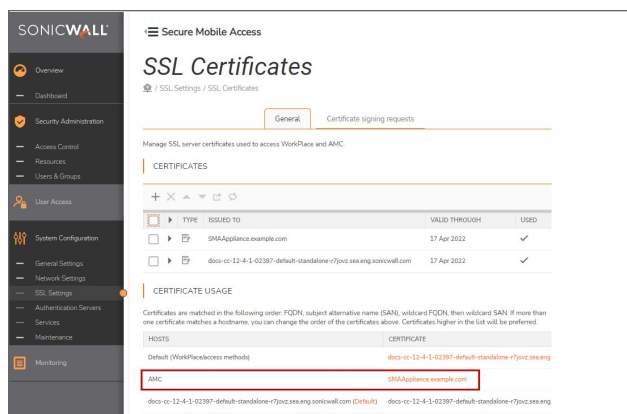
- When generating an EC key, from the **Prime size** list, select a size:

- **256 bits:** selects the P-256 curve.
- **384 bits:** selects the P-384 curve.

❗ | **NOTE:** 4096-bit keys were not evaluated or tested during the evaluation.

7. Click **Save**.
8. Securely transfer the new certificate request to the trusted Certificate Authority for signing.  
❗ | **NOTE:** The Certificate Signing request includes ----- BEGIN and ----- END lines, and is typically a .csr or .pem binary file.
9. Receive signed certificate back from a trusted Certificate Authority (CA).
10. Navigate to **System Configuration > SSL Settings**.
11. Next to **SSL Certificates**, click **Edit**.
12. Click **Certificate Signing Request**.

13. Click **Process CSR Response** next to the name of the newly created Certificate Signing Request.
14. Securely upload the signed certificate request.
  - ① **NOTE:** A signed certificate includes ----- BEGIN CERTIFICATE and ----- END CERTIFICATE lines, and is typically a .pem binary file.
15. Click **Save**.
16. In the **Certificate Usage** section, next to **AMC**, confirm that the new certificate is selected.

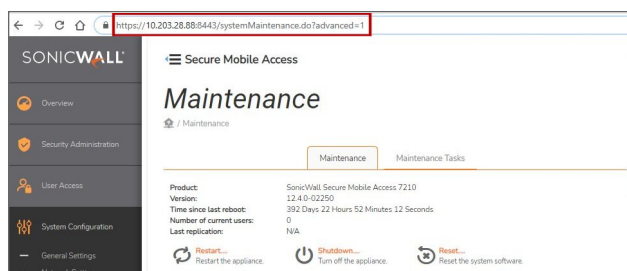


17. Click **Pending Changes** to apply these configuration changes

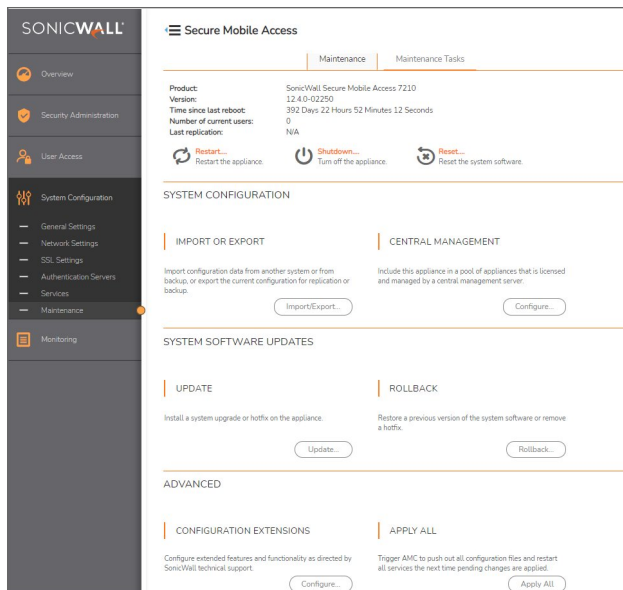
## Configure TLS Settings

*To configure the TLS settings:*

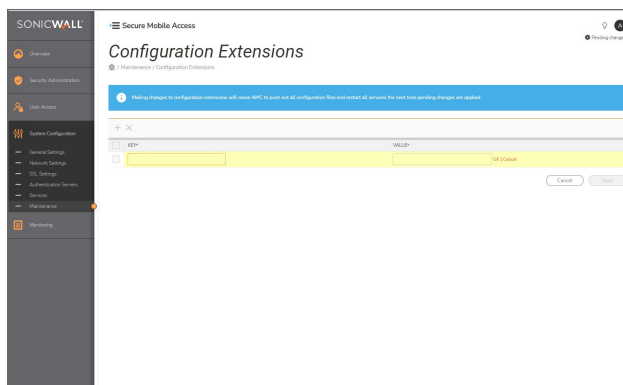
1. Navigate to **System Configuration > Maintenance**.
2. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.



3. Scroll down to the **Advanced > Configuration Extensions** section.

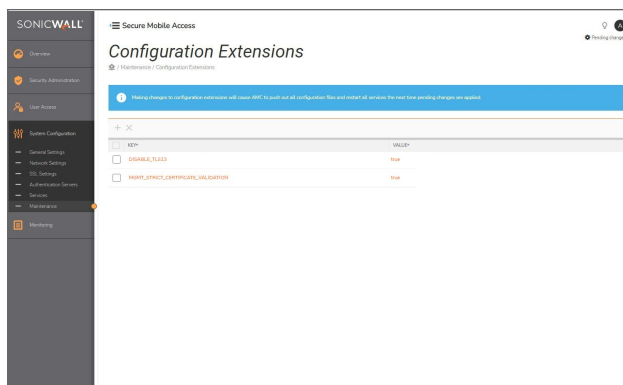


4. On the **Configuration Extensions** page, click the New (+) icon.



5. In the table:
  - For the **Key** enter `MGMT_STRICT_CERTIFICATE_VALIDATION`, for the **Value** enter `true`, and click **OK**.
  - For the **Key** enter `DISABLE_TLS13`, for the **Value** enter `true`, and click **OK**.



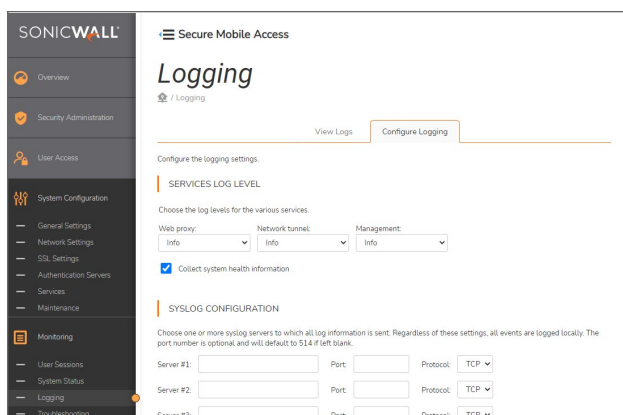


6. Click **Save**.
7. Click **Pending Changes** to apply these configuration changes.
8. Navigate to **System Configuration > SSL Settings**.
9. Next to **SSL Encryption**, click on **Edit**.
10. In the **Security Level** section, select **Secure**.
  - ① | **IMPORTANT:** Only select **Secure** for this setting.
11. Click **Save**.
12. Click **Pending Changes** to apply these configuration changes

## Configure Audit Policy

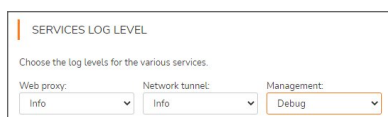
*To configure the audit policy:*

1. Navigate to **Monitoring > Logging**.



- 2.
3. Click **Configure Logging**.

4. In the **Service Log Level** section:
  - a. Verify that **Web proxy** and **Network tunnel** log levels are set to **Info**.
  - b. From the **Management** list, select **Debug**.



SERVICES LOG LEVEL

Choose the log levels for the various services.

Web proxy: Info Network tunnel: Info Management: Debug

5. Click **Save**.

## Configure External Audit Server (Syslog)

### *To configure an external audit server:*

1. Navigate to **System Configuration > SSL Settings**.
2. In the **CA Certificates** section, click **Edit** next to the number of certificates.
3. Click the New (+) icon.
4. Select **Certificate file**.
5. Click **Choose File**.
6. Navigate to and select the CA certificate issued by syslog server.
7. In the **Usage** section, select **OCSP response verification**.
8. Click **Import**.
9. Click **Pending Changes** to apply these configuration changes.
10. When the **Apply Pending Changes** dialog displays, click **Apply Changes**. All pending changes will be applied to the appliance.
11. Click **Close**.
12. Navigate to **Monitoring > Logging**.
13. Click **Configure Logging**.
14. In the **Syslog Configuration** section, enter the IP address and port number of a syslog server.
15. From the **Protocol** list, select **TLS**.

16. Click **Save**.
17. Click **Pending Changes** to apply these configuration changes.

## Topics:

- [Certificate Requirements](#)
- [Troubleshooting](#)

# Certificate Requirements

Several checks are performed when connecting to a remote syslog server using TLS.

X509v3 Attribute	Required value
<b>extendedKeyUsage</b>	serverAuth
<b>subjectAltName</b>	A list of hostnames or IP addresses that the certificate is valid for. If the configured syslog server name does not appear in this list, then the connection is rejected. See RFC6125 for details.
	<div> <div></div> <div><b>NOTE:</b> Deploying a certificate with an IP address in the certificate is <b>highly</b> discouraged.</div> </div>
<b>notValidBefore / notValidAfter</b>	Standard expiration checks
<b>basicConstraints</b>	The CA basic constraint must be <b>FALSE</b>
<b>Subject name</b>	The <code>MGMT_CSFC_CERTIFICATE_REQUIRED_OUTBOUND_ATTRIBUTES</code> CEM extension can be used to require an attribute to have a certain value. Please see documentation of <code>MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES</code> in <a href="#">Configure TLS Mutual Authentication</a> for details on the format.
<b>authorityInfoAccess</b>	An OCSP URL must be specified. The OCSP status of the certificate is checked during initial TLS handshake. If anything other than a <code>GOOD</code> status is received, the connection will be rejected.

A valid certificate would look like this (results of `openssl x509 -in FILENAME.CERT -noout -text`):

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
0a:a5:c8:97:83:3f:27:e0:44:20:53:0e:18:4b:cf:b3:7e:91:54:4f
Signature Algorithm: sha384WithRSAEncryption
Issuer: C = US, ST = Washington, L = Seattle, O = SonicWall, OU = Engineering, CN =
Testing Intermediate CA
Validity
    Not Before: Feb 17 17:43:19 2021 GMT
    Not After : Feb 28 17:43:19 2021 GMT
Subject: C = US, ST = Washington, L = Seattle, O = SonicWall, OU = Engineering, CN =
172.16.1.101
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus: [....]
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:FALSE
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Subject Alternative Name: critical
        DNS:foo.bar.com
    Authority Information Access:
        OCSP - URI:http://172.16.1.101:65290/OCSP

    X509v3 Subject Key Identifier:
        F3:70:38:40:55:46:87:14:D4:95:EA:F0:D5:79:9D:09:B6:76:7C:7A
    X509v3 Authority Key Identifier:
        keyid:9F:4D:57:A6:6B:31:C3:F4:85:B5:71:A3:D1:FD:66:75:21:5F:D9:A7

Signature Algorithm: sha384WithRSAEncryption [...]
```

# Troubleshooting

If messages from the SMA appliance are not appearing on the remote syslog server, it usually indicates a configuration problem relating to the certificate. Relevant messages would be in `/var/log/syslog`. Most frequent errors and their solutions include:

Message	Solution
<b>syslog-ng: Certificate subject does not match configured hostname;</b> <b>subject='/C=US/ST=Washington/L=Seattle/O=SonicWall/OU=Engineering/CN=172.16.1.101',</b> <b>hostname='172.16.1.101',</b> <b>certificate='syslog.example.com'</b>	The SAN of the certificate on the syslog server does not match the hostname configured in the AMC. Make sure that the hostname used in the AMC syslog configuration is a hostname (not an IP address) and is a name that is included in the SAN list.
<b>syslog-ng: TLS handshake failure - no mutually acceptable protocol could be negotiated source (172.16.1.77:1171) destination (172.16.1.101:9999);</b>	The syslog server rejected the TLS handshake. Make sure that the remote syslog server accepts TLS1.2 or TLS1.3 connections.
<b>syslog-ng: TLS handshake failure - no mutually acceptable cipher could be negotiated source (172.16.1.77:1171) destination (172.16.1.101:9999);</b>	The syslog server rejected the TLS handshake. Make sure that the remote syslog server accepts ECDHE cipher suites.
<b>syslog-ng: X509_NAME outbound attribute mismatch (countryName) - expected(CA) subject (/C=US/ST=Washington/L=Seattle/O=SonicWall/OU=Engineering/CN=172.16.1.101);</b>	The certificate subject did not contain the proper attributes. Please check the <code>MGMT_CSFC_CERTIFICATE_REQUIRED_OUTBOUND_ATTRIBUTES</code> setting.

## Configure TLS Mutual Authentication

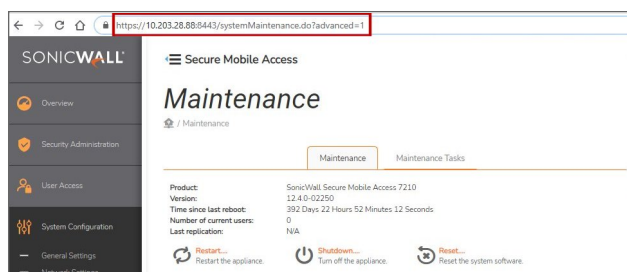
For more information on configuration TLS mutual authentication ("PKI authentication"), refer to "Configuring a PKI Authentication Server" in the *Secure Mobile Access 12.4 Administration Guide*.

① **NOTE:** To use mutual authentication on an authentication server as well, an authentication realm must be configured on the appliance.

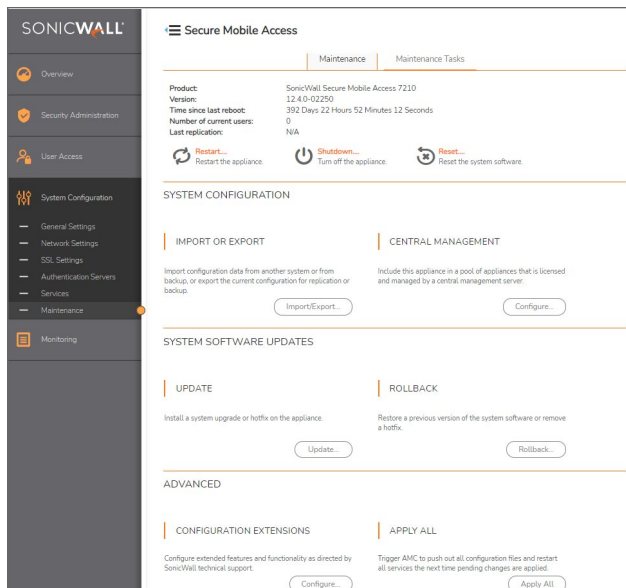
### To configure TLS mutual authentication:

1. Login to the AMC.
2. Navigate to **System Configuration > Authentication Servers**.
3. In the **Authentication Servers** section, click **New**.

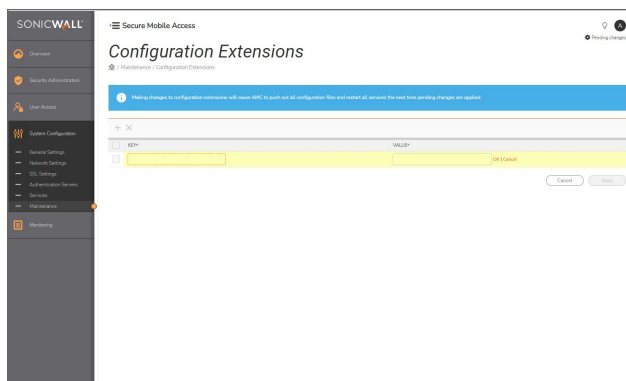
4. On the **Add Authentication Server** page:
  - a. In the **User Store** section, under **Authentication directory**, select **Public key infrastructure (PKI)**.
  - b. Under **Credential Type**, select **Digital Certificate**.
  - c. Click **Continue**.
  - d. In the Name field, provide a name for the server for easy reference later, such as *Certificates*.
  - e. Select the certificate authorities you wish to trust for mutual authentication in the pick-list on the left pane (**All CA Certificates**) and click the checkmark. The CAs will be moved into the right pane (**Trusted CA Certificates**).
  - f. Click to expand the **Advanced** section.
    1. Enable **Use OCSP to verify client certificates**.
    2. Enable **User certificate's AIA extension**.
    3. Disable **Allow certificate if responder is unavailable**.
    4. Enable **Verify response**.
5. Click **Save**.
6. Navigate to **User Access > Realms**.
7. Click **+ New realm** at the upper right of the page.
8. On the **Configure Realm** page:
  - a. Provide a name for the realm to be displayed to the user ("Client Certificates")
  - b. Enable the checkbox next to Display this realm
  - c. Select the authentication server in the dropdown for Authentication server
  - d. Click **Finish**.
9. Navigate to **System Configuration > Maintenance**.
10. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.



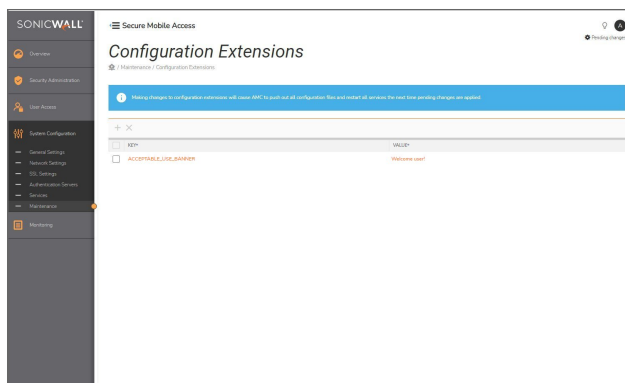
11. Scroll down to the **Advanced > Configuration Extensions** section.



12. Click **Configure...**
13. On the **Configuration Extensions** page, click the New (+) icon.



14. In the table:
  - For the **Key** enter `MGMT_CSFC_CERTIFICATE_VALIDATION`, for the **Value** enter `true`, and click **OK**.
  - For the **Key** enter `MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES`, for the **Value** enter at least one attribute and a required value that must be present in all certificates that should be accepted for client authentication.



15. Click **Save**.
16. Click **Pending Changes** to apply these configuration changes.
17. Click on “New” button.
18. Add a new parameter `MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES`
19. In the value field, enter at least one attribute and a required value that must be present in all certificates that should be accepted for client authentication.
  - Different key/value pairs should be delimited with the literal `&&`. For example: to require that all certificates are issued from a trusted CA and also have an `organizationName` of SonicWall and an `organizationalUnitName` of Engineering , you would use `MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES=O=SonicWall && OU=Engineering`
  - Either the short or long name of an attribute may be used (`O` instead of `organizationName`, `OU` instead of `organizationalUnitName`). In logs, only the long name will be used.
  - Supported attributes:
    - `countryName / C`
    - `organizationName / O`
    - `organizationalUnitName / OU`
    - `stateOrProvinceName / ST`
    - `commonName / CN`
    - `serialNumber`
    - `locality / L`
    - `title`
    - `surName / SN`
    - `givenName / GN`
    - `pseudonym`
    - `generationQualifier`

Click **OK**.



20. Click **Save**.
21. Click **Pending Changes** to apply these configuration changes.

After these steps, the **Client Certificates** option will be available in the authentication sequence (for both web access methods and tunnel clients).

① **NOTE:** When using client certificates for a realm, **only** client certificates can be used to authenticate for that realm. If you wish to have a 'fallback' authentication for when someone does not have a client certificate, that requires a separate authentication server and realm. Please refer to the online documentation for details.

## Set Other Useful Web Security Options

There are other web security options you might want to set as well, depending on your environment.

### Topics:

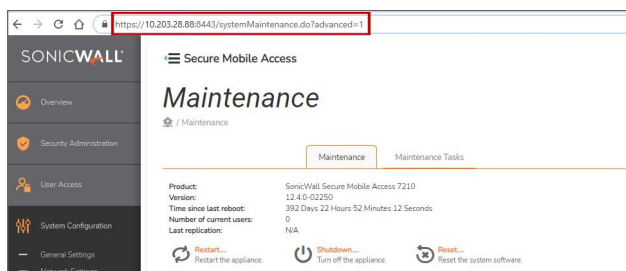
- [Forcing the use of the HTTPS Protocol](#)
- [Preventing the Display of Embedded Web Content](#)

## Forcing the use of the HTTPS Protocol

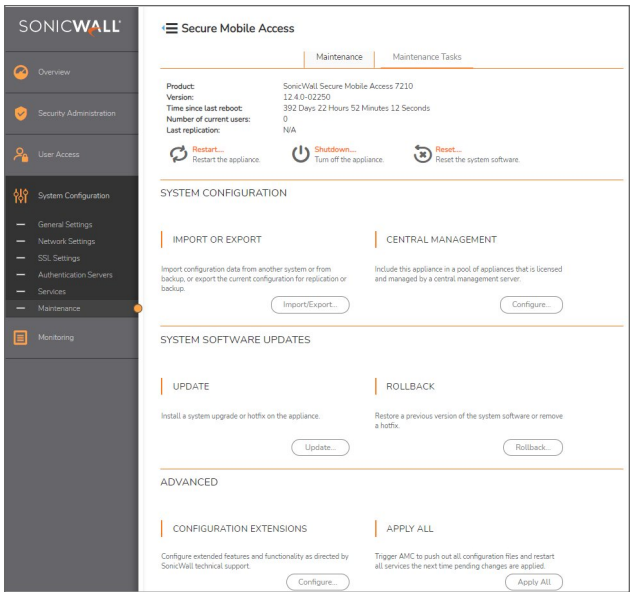
You can force clients to only use the HTTPS protocol to connect to the appliance. All HTTP traffic is automatically redirected to HTTPS, but setting this option prevents a client from even attempting to communicate without encryption if a user manually types in a URL such as `http://vpnsrv.com/`.

### *To enable force the usage of the HTTPS protocol:*

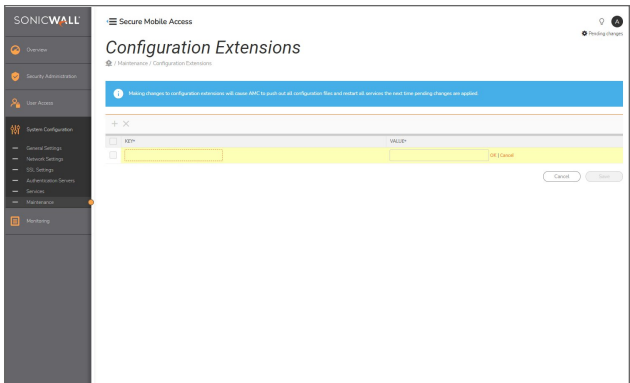
1. Navigate to **System Configuration > Maintenance**.
2. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.



3. Scroll down to the **Advanced > Configuration Extensions** section.

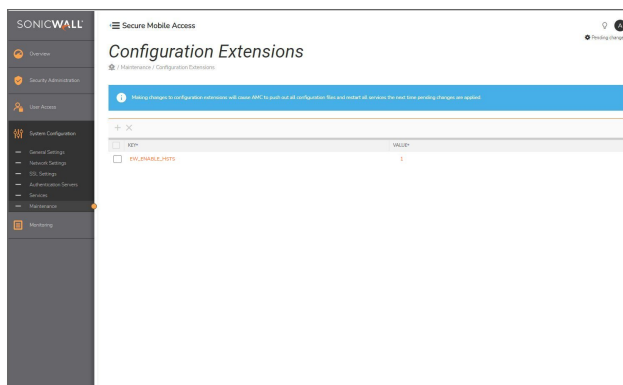


4. On the **Configuration Extensions** page, click the New (+) icon.



5. In the table:

- For the **Key** enter `EW_ENABLE_HSTS`, for the **Value** enter `1`, and click **OK**.



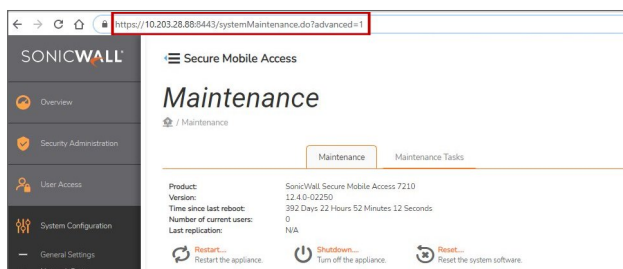
6. Click **Save**.
7. Click **Pending Changes** to apply these configuration changes.

## Preventing the Display of Embedded Web Content

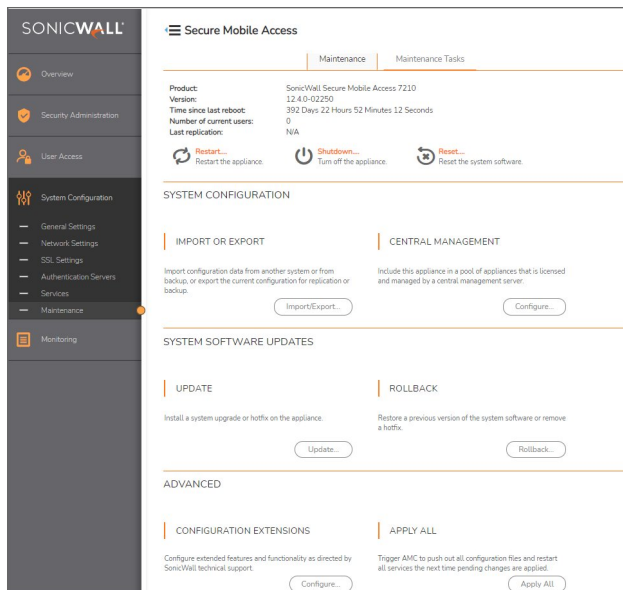
You can prevent common "clickjacking" attacks by not allowing any web pages to be embedded with in a `<frame>` inside of an attacker's page.

### *To block embedded web pages:*

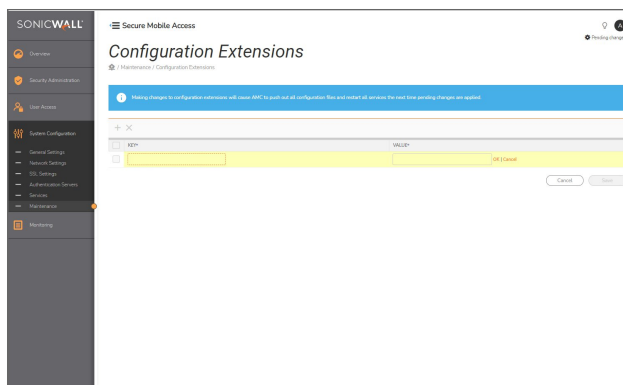
1. Navigate to **System Configuration > Maintenance**.
2. In your web browser, modify the URL by appending a query parameter `?advanced=1` and press Enter.



3. Scroll down to the **Advanced > Configuration Extensions** section.

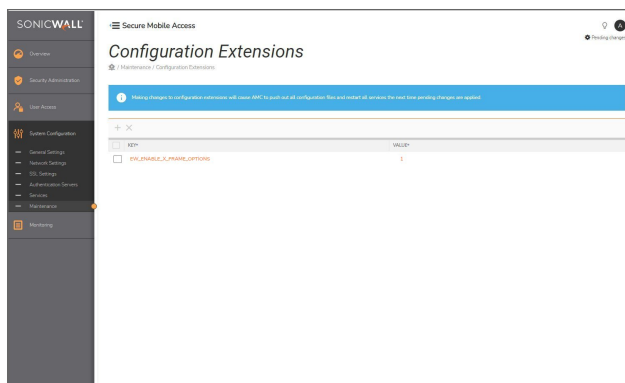


4. On the **Configuration Extensions** page, click the New (+) icon.



5. In the table:

- For the **Key** enter `EW_ENABLE_X_FRAME_OPTIONS`, for the **Value** enter `1`, and click **OK**.

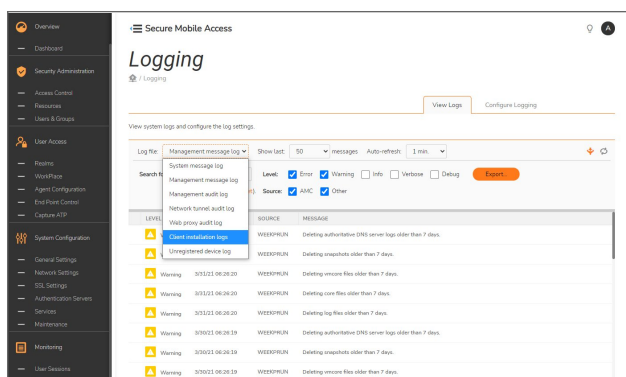


6. Click **Save**.
7. Click **Pending Changes** to apply these configuration changes.

# Auditable Events

To access audit records through the AMC:

1. Navigate to **Monitoring > Logging > View Logs**.



Each audit record contains this information:

- type of event (**Level**)
- date and time of the event (**Time**)
- subject identity (**Source**)
- outcome (**Message**)

LEVEL	TIME	SOURCE	MESSAGE
Warning	3/31/21 06:26:20	WEEKPRUN	Deleting authoritative DNS server logs older than 7 days.

The audit records may also contain event-specific content.

The SMA supports these audit events levels:

- **Fatal**
- **Error**
- **Warning**
- **Info**

- Verbose
- Debug

The following auditable events are in the scope of Common Criteria certification:

Auditable Actions	Audit Records
<b>Start-up and shut down of audit functions</b>	<p><b>Start-up:</b></p> <p>Aug 6 15:30:50 SMAAppliance boot-process: System has successfully booted.</p> <p><b>Shut down:</b></p> <p>Info 6/21/21 15:39:19 admin shutdown the system</p>
<b>Change of audit level</b>	<p>Info 8/2/21 12:27:53 admin Updated logging settings - Name=loggingServiceLogLevel Value=info</p> <p>Info 8/2/21 12:35:17 admin Updated logging settings - Name=loggingServiceLogLevel Value=verbose</p> <p>Info 8/2/21 12:27:49 admin Updated logging settings - Name=loggingServiceLogLevel Value=warning</p> <p>Info 8/2/21 12:27:45 admin Updated logging settings - Name=loggingServiceLogLevel Value=error</p> <p>Info 8/2/21 12:27:32 admin Updated logging settings - Name=loggingServiceLogLevel Value=fatal</p> <p>Info 8/2/21 12:27:58 admin Updated logging settings - Name=loggingServiceLogLevel Value=debug</p>
<b>Configure RBAC mode</b>	<p>Info 9/11/21 13:48:17 admin Added administrator account - Username= user1 Role= Super Admin</p>
<b>Configure password complexity</b>	<p>Info 8/27/21 12:05:17 admin Updated authentication server - ID=AV1565090969028AUI Name=local Password length=12-16 Require lowercase=false Require uppercase=true Require digits=true Require symbols=false</p>

Auditable Actions	Audit Records
<b>TLS configuration</b>	<p>Info 8/2/21 16:44:01 admin Deleted SSL protocol - Name=TLSv1</p> <p>Info 8/2/21 16:41:52 admin Added SSL protocol - Name=TLSv1_2</p> <p>Info 8/2/21 16:45:46 admin Deleted SSL cipher - Name=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</p> <p>Info 8/2/21 16:45:46 admin Changed order of SSL cipher - Name=TLS_RSA_WITH_AES_256_GCM_SHA384 From=2 To=0</p>
<b>FIPS mode</b>	<p>Info 6/20/21 13:21:25 admin Updated FIPS settings - Enabled=true</p> <p>Info 6/20/21 13:35:46 admin Updated FIPS settings - Enabled=false</p>
<b>Audit server configuration</b>	<p>Info 8/2/21 16:53:59 admin Updated syslog settings: Server1=10.5.252.101:9999/tcp Server2=None Server3=None</p>
<b>X.509 Certificate management</b>	<p><b>Certificate Authority (CA)</b></p> <p>Info 8/8/21 09:25:19 admin Added CA certificate - Issued to=ROOTCA</p> <p>Info 8/8/21 09:25:04 admin Deleted CA certificate - Issued to=ROOTCA</p> <p><b>Certificate Signing Request (CSR)</b></p> <p>Info 6/12/21 15:40:13 admin Added SSL certificate signing request - Issued to=example.sonicwall.com</p> <p>Info 8/8/21 10:20:23 admin Added SSL certificate - Issued to= example.sonicwall.com</p> <p>Error 6/26/27 11:36:48 AMC unable to import CSR reply: Failed signature verification</p> <p>Error 6/26/27 11:35:39 AMC unable to import CSR reply:java.io.IOException: Incomplete BER/DER data</p>

#### Certificate Authority (CA)

The entity that verifies the contents of the digital certificate and signs it indicating that the certificate is valid and correct is called the Certificate Authority (CA).

#### Certificate Signing Request (CSR)

An entity that wants a signed certificate or a digital certificate requests one through a CSR.



Auditable Actions	Audit Records
Verifying and applying updates	<p>Uploading a Valid hotfix file:</p> <pre>Info 6/24/21 10:47:57 admin Installed hotfix pform-hotfix-12.1.0-06163</pre>
	<p>Uploading an Invalid hotfix file:</p> <pre>Error 8/2/21 17:36:15 admin Hotfix update failed: Hotfix file integrity check failed.</pre>
Configuring system time	<pre>Info 6/12/21 12:59:17 admin Set time to Wed Jun 12 12:59:17 IST 2019</pre>
Configuring and modifying access banner	<pre>Info 6/23/21 11:57:32 admin Updated acceptable use banner</pre>
Configuring termination of interactive remote session	<pre>Info 8/2/21 18:05:18 admin Added configuration extension - Key=AMC_SESSION_TIMEOUT_SECS Value=30</pre>
Operations related to cryptographic keys or certificates	<p>Commands to delete TOE's identity (i.e. web) certificate:</p> <pre>Info 8/5/21 09:21:01 admin Added SSL certificate - Issued to=192.168.0.10  Info 8/5/21 09:21:07 admin Updated SSL certificate - Usage=AMC Issued to=192.168.0.10  Info 8/5/21 10:02:36 admin Deleted SSL certificate - Issued to=172.29.0.204</pre>
	<p>Commands to delete trusted CA:</p> <pre>Info 8/5/21 10:08:07 admin Deleted CA certificate - Issued to=Unit Testing CA</pre>

Auditable Actions	Audit Records
<b>Administrative login</b>	<p data-bbox="716 266 1062 291"><b>Successful administrative login:</b></p> <p data-bbox="716 321 1328 378">Info 6/11/21 09:00:14 admin Login succeeded - Address=10.1.101.10</p> <p data-bbox="716 405 1089 430"><b>Unsuccessful administrative login:</b></p> <p data-bbox="716 459 1300 516">Warning 6/11/21 06:26:28 AMC Authentication failed: Username=admin, Address=10.1.101.10</p> <p data-bbox="716 543 1284 569"><b>Unsuccessful login attempt limit is met or exceeded:</b></p> <p data-bbox="716 598 1356 686">Info 7/25/21 14:52:50 admin Added configuration extension - Key=ADMINISTRATOR_ACCOUNT_LOCKOUT_SECONDS Value=180</p> <p data-bbox="716 716 1356 804">Info 7/25/21 14:52:50 admin Added configuration extension - Key=ADMINISTRATOR_ACCOUNT_LOCKOUT_ATTEMPTS Value=4</p> <p data-bbox="716 833 1273 924">Error 8/5/21 11:58:13 admin Administrator account locked due to 3 successive login failures</p> <p data-bbox="716 951 1149 976"><b>Timeout of local administrative session:</b></p> <p data-bbox="716 1005 1295 1062">Sep 3 15:55:04 SMAAppliance -bash: Timeout, session closed for user(root)</p> <p data-bbox="716 1092 1328 1180">Sep 3 15:55:04 SMAAppliance login[4754]: pam_unix(login:session): session closed for user root</p> <p data-bbox="716 1207 1175 1232"><b>Timeout of remote administrative session:</b></p> <p data-bbox="716 1262 1356 1318">Logout - Address=192.168.56.1 Duration=03:15:57 Expired=true</p> <p data-bbox="716 1346 992 1371"><b>Administrator logging off:</b></p> <p data-bbox="716 1400 1219 1491">Info 6/21/21 13:24:57 admin Logout - Address=10.5.22.125 Duration=00:00:26 Expired=false</p>

Auditable Actions	Audit Records
Account management	Creation of a new user:
	Info 6/24/21 19:32:12 admin Added administrator account - Username=user1
	Disabling of user account by administrative action:
	Info 8/26/21 12:26:15 admin Updated local user - ID=AV1565098985406CPP Name=user1 Password changed=false Enabled=false
	Deletion of existing account:
	Info 6/24/21 20:12:34 admin Deleted administrator account - ID=AV1561384932759GQT Username=user1
	Reset of User Password:
	Info 8/6/21 19:07:46 admin Updated administrator account - ID=PrimaryAdmin Username=admin Role=Primary Admin Password changed=true
Failure to establish a TLS session	Error 6/24/21 15:41:31 AMC SSL handshake failed: Client requested protocol TLSv1 not enabled or not supported.
	Error 6/25/21 15:26:35 AMC SSL handshake failed: no cipher suites in common
Unsuccessful attempt to validate an X509 certificate	Aug 8 18:56:24 syslog-ng@SMAAppliance syslog.err syslog-ng: Certificate subject does not match configured hostname; subject='/DC=com/DC=smal000/CN=ROOT', hostname='10.1.111.101', certificate='ROOT'

# Configuring TLS Certificates on the Client

① | **NOTE:** These instructions only apply to Windows 10 clients.

*To configure TLS certificates on a client:*

1. Open the Microsoft Management Console (MMC): **Start > Run > MMC**.
2. Select **File > Add / Remove Snap In**.
3. Double click **Certificates**.
4. Select **My user account**.
5. Click **Finish**.
6. Click **OK**.
7. Expand **Certificates > Personal > Certificates**.
8. Right click on **Certificates** and select **All Tasks > Import**.
9. Click **Next**.
10. Click **Browse**.
11. Navigate to and select the certificate you would like to import.
12. Click **Open**.
13. Click **Next**.
14. Enter the **Password**.
15. Click **Next**.
16. Click **Next**.
17. Click **Finish**.
18. Click **OK**.

Follow the preceding steps to import CA certificates into Trusted Stores. Select the certificate store:

- Intermediate Certification Authorities for importing intermediate certificates
- Trusted Root Certification Authorities for importing root certificates

# Client Certificate Validation

A client certificate is validated when it is presented during the initial TLS handshake.

The validation process consists of these phases:

1. Certificate authority validation – is the certificate signed by one of the certificate authorities that the SMA appliance is configured to trust?
2. Expiration validation – is the certificate still within its `notValidBefore` and `notValidAfter` window?
3. OCSP validation – Does the certificate have an `authorityInfoAccess` attribute, and does the OCSP server return a `GOOD` response for it? If there is no OCSP server set, it responds with an error, or responds with `unknown` or `revoked` status, the certificate is rejected.

These checks are performed for all certificate authorities in the chain.

The client certificate itself must also contain the `clientAuth` extendedKeyUsage attribute. The `MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES` CEM extension can be used to require an attribute to have a certain value. Refer to [Configure TLS Mutual Authentication](#) for details on the format required for `MGMT_CSFC_CERTIFICATE_REQUIRED_ATTRIBUTES`.

# Certificate Types

There are two different roles for certificates that are used in the SMA appliance firmware. The super admin may generate, import, export, or delete certificates and assign them to different roles. A certificate cannot be edited to change its attributes after it has been generated or imported.

Certificates may be managed by:

1. Logging in to the AMC.
2. Navigate to **System Configuration > SSL Settings**.
3. Next to **SSL Certificates**, click **Edit**.

Roles for certificates may be changed by modifying the list of **Hosts** under the **Certificate Usage** heading.

- A single certificate may be selected for **AMC**: this certificate will be used for TLS communications on port 8443 of the management interface
- All other certificates will be used by the remote access methods (Workplace, Tunnel, etc).
  - During the TLS handshake the `serverNameIndicator` extension from the client will be used to find an appropriate certificate. If a certificate has a `subjectAlternateName` (IP or DNS) entry that matches the `serverNameIndicator`, it will be used. The most specific match will be used – the certificate for `vpn.xyzzzy.com` will be used before `*.xyzzzy.com`.
  - If no match is found, or no `serverNameIndicator` extension was present, then the default certificate will be used (“Default (WorkPlace/access methods)”).

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Secure Mobile Access Common Criteria Configuration Guide

Updated - September 2021

Software Version - 12.4

232-005623-00 Rev 1.2

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

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

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