

SonicWall SMA v12.1 Configuration for Common Criteria

**Version 0.5
June 24, 2020**



Copyright © 2019 SonicWall. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. SonicWall™ and SonicWall logo are trademarks of SonicWall in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

1 INTRODUCTION 3

1.1 ABOUT THIS DOCUMENT 3

1.2 OTHER RELATED DOCUMENTS 3

1.3 ABOUT SMA 3

 1.3.1 *Target of Evaluation* 3

 1.3.2 *Description* 3

 1.3.3 *Management Interfaces* 4

 1.3.4 *Physical Interfaces* 4

1.4 ASSUMPTIONS 4

2 COMMON CRITERIA CONFIGURATION 6

2.1 INITIAL ACCESS AND NETWORK CONFIGURATION 6

2.2 SETUP WIZARD 8

2.3 ACCESSING SECURE MOBILE ACCESS MANAGEMENT CONSOLE 11

2.4 EVALUATED CONFIGURATION 13

3 AUDITABLE EVENTS 28

Figures and Tables

FIGURE 1: SMA INTERFACES 4

TABLE 1: OTHER RELATED DOCUMENTS 3

TABLE 2: PLATFORMS AND DEVICES 3

TABLE 3: ASSUMPTIONS 4

1 Introduction

1.1 About This Document

This guide provides the information needed to set up SonicWall Secure Mobile Access v12.1 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 SonicWall Secure Mobile Access 12.1 Administration Guide and SonicWall Secure Mobile Access 6210/7210 Getting Started Guide.

1.2 Other Related Documents

Table 1: Other Related Documents

Item	Identifier	Short Form
Security Target	SonicWALL SMA 12.1 Security Target v0.7	ST
Protection Profile	collaborative Protection Profile for Network Devices Version 2.1, 24 September 2018 (NDcPP)	NDcPP
Administration Guide	SonicWall Secure Mobile Access 12.1 Administration Guide	ADMIN
Getting Started Guide	SonicWall Secure Mobile Access 6210/7210 Getting Started Guide	START

1.3 About SMA

1.3.1 Target of Evaluation

Developer: SonicWall

Identification: SonicWall Secure Mobile Access (SMA) v12.1

Table 2: Platforms and Devices

Series	Platforms	Build
SonicWall Secure Mobile Access	SMA 6210	12.1.0-05477
	SMA 7210	

Claimed Protection Profile: collaborative Protection Profile for Network Devices v2.1.

1.3.2 Description

The SonicWall Secure Mobile Access (SMA) v12.1 in the evaluated configuration consists of SMA 6210 and SMA 7210 appliances. 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).

1.3.3 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 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.

1.3.4 Physical Interfaces

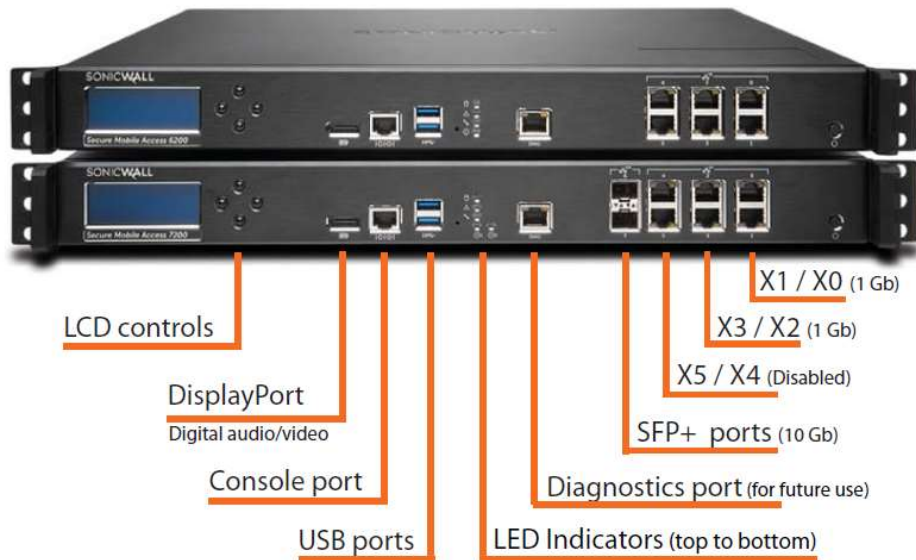


Figure 1: SMA Interfaces

1.4 Assumptions

This section identifies assumptions as specified in the NDcPP.

Table 3: Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL_PROTECTION	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.

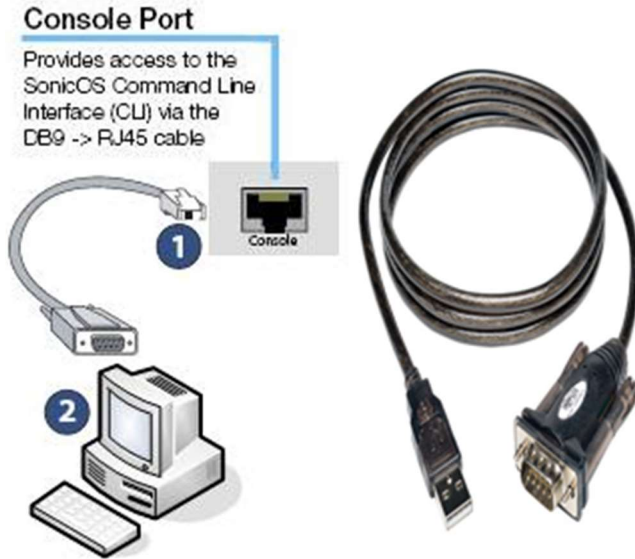
SonicWall SMA v12.1

Assumption Name	Assumption Definition
A.LIMITED_FUNCTIONALITY	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 computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	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).
A.TRUSTED_ADMINISTRATOR	<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 passwords/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>
A.REGULAR_UPDATES	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.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	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 networking equipment when the equipment is discarded or removed from its operational environment.

2 Common Criteria Configuration

2.1 Initial access and network configuration

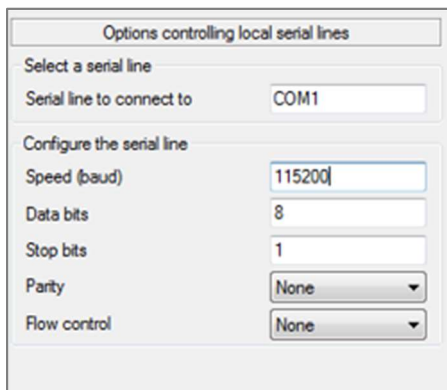
Attach the included null modem cable to the appliance port marked **Console Port** (See Figure 1). Attach the other end of the null modem cable to a serial port of the management workstation computer.



Launch a terminal emulation application that support serial port communications, for example PuTTY or HyperTerminal.

Use these serial line settings:

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



SonicWall SMA v12.1

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: █
```

- At the **login:** prompt enter the administrator's username. The default Admin username is **root**. Once SMA is fully configured, the root account should be disabled.
- At the **Password:** prompt, enter the root password. If an invalid or mismatched username or password are entered, the CLI prompt will return to **login:** prompt and a "*CLI administrator login denied due to bad credentials*" error message will be logged.

On initial login, SMA appliance will initiate initial configuration prompt as shown below:

```
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] █
```

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
```

SonicWall SMA v12.1

Once the interfaces are configured you will see the conformation as below.

```
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]
```

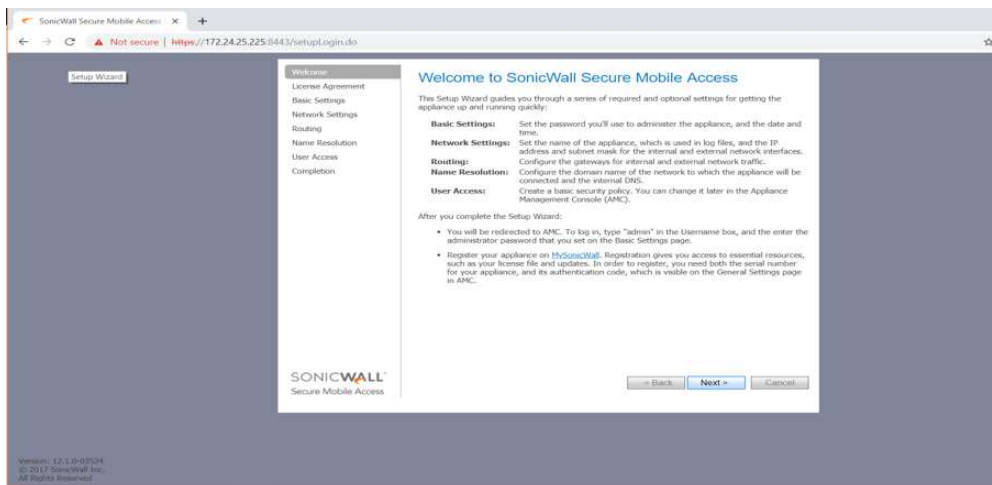
To terminate CLI session, type `logout`

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

2.2 Setup Wizard

Access SMA via a browser by typing url: “<https://<IP address>:8443>” (where <IP address> matches the address configured in the previous section). *Note: The default internal IP address is 192.168.0.10*

Once initially connected, you will interact with a setup wizard to configure the external interfaces and other initial configurations.



SonicWall SMA v12.1

In the following **Basic Settings** page specify the admin password and select the time zone:

Version: 12.1.0-03524
© 2017 SonicWall Inc.
All Rights Reserved

In the following **Network Settings** page specify the corresponding external IP and Subnet mask for the external IP specified and click next to navigate to next page.

Version: 12.1.0-03524
© 2017 SonicWall Inc.
All Rights Reserved

SonicWall SMA v12.1

In the following **Routing** page specify the external gateway IP. Internal gateway IP will be pre-filled as it was already configured in the AMC setup tool. Click next to navigate to next page.

The screenshot shows the 'Routing' configuration page in the SonicWall SMA v12.1 interface. The left sidebar contains a navigation menu with options: Welcome, License Agreement, Basic Settings, Network Settings, Routing, Name Resolution, User Access, and Completion. The 'Routing' section is active. The main content area is titled 'Routing' and contains the following text: '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.' Below this, it states: 'If you plan to access AMC from a computer on a different subnet than the appliance (172.29.0.98/255.255.0.0), you must configure an external 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.' The 'Routing mode' is set to 'Dual gateway'. The 'Internal gateway IP address' is pre-filled with '172.24.0.1'. The 'External gateway IP address' is '10.5.114.1'. There are two explanatory text blocks: one for the internal gateway stating it must be on the same subnet as the internal interface (172.29.0.98/255.255.0.0), and one for the external gateway stating it must be on the same subnet as the external interface (10.5.114.98/255.255.0.0). At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The SonicWall logo and 'Secure Mobile Access' text are at the bottom left. A footer at the bottom left reads: 'Version: 12.1.0-03524 © 2017 SonicWall Inc. All Rights Reserved.'

In the following **Name Resolution** page, enter Default domain and primary DNS server IP and click on Next.

The screenshot shows the 'Name Resolution' configuration page in the SonicWall SMA v12.1 interface. The left sidebar contains a navigation menu with options: Welcome, License Agreement, Basic Settings, Network Settings, Routing, Name Resolution, User Access, and Completion. The 'Name Resolution' section is active. The main content area is titled 'Name Resolution' and contains the following text: '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, it states: 'The domain in which the appliance is located (such as example.com)'. The 'Default domain' is 'test'. The 'DNS Server' is empty. There is a text box for the DNS server with the instruction: 'Enter the IP address for your primary DNS server. More DNS servers can be added later in AMC.' At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The SonicWall logo and 'Secure Mobile Access' text are at the bottom left. A footer at the bottom left reads: 'Version: 12.1.0-03524 © 2017 SonicWall Inc. All Rights Reserved.'

In the following **User Access** page specify the NAT address and Access policy. This option is not mandatory and can be skipped to be configured later.

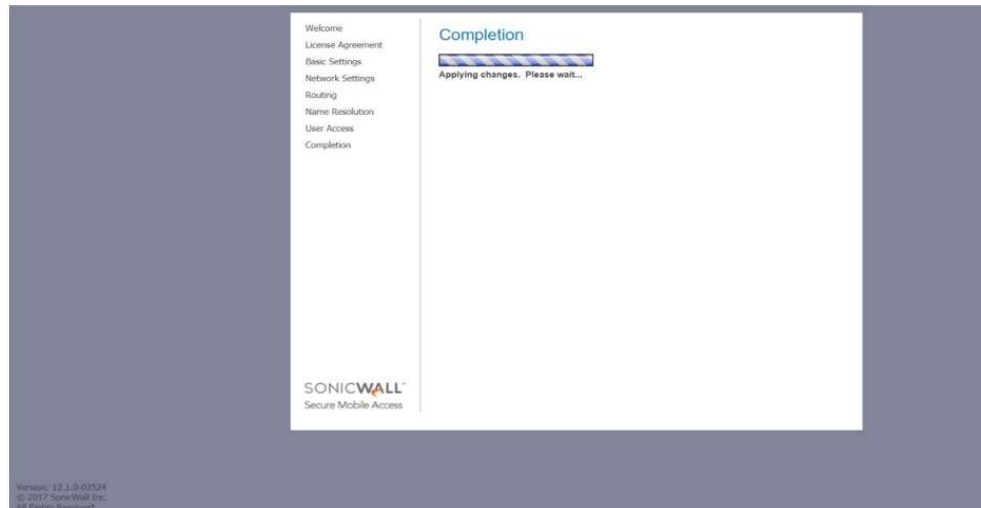
The screenshot shows the 'User Access' configuration page in the SonicWall SMA v12.1 interface. The left sidebar contains a navigation menu with options: Welcome, License Agreement, Basic Settings, Network Settings, Routing, Name Resolution, User Access, and Completion. The 'User Access' section is active. The main content area is titled 'User Access' and contains the following text: '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, it states: 'Enable full network access using OnDemand Tunnel'. The 'NAT address for network tunneled traffic' is '172.24.0.1'. There is a text box for the NAT address with the instruction: 'The NAT address for network tunneled traffic must be on the same subnet as the internal interface (172.24.0.98/255.255.0.0)'. Below this, it states: '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'. Below these, it states: 'Initially deny all access' and 'Create access rules that deny access. Granular access to specific resources can be defined later in AMC.' At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The SonicWall logo and 'Secure Mobile Access' text are at the bottom left. A footer at the bottom left reads: 'Version: 12.1.0-03524 © 2017 SonicWall Inc. All Rights Reserved.'

SonicWall SMA v12.1

In the following **Completion** page you can review all configured settings. If all the presented information is correct click on Finish or you can go back by clicking Back and change any of the settings.

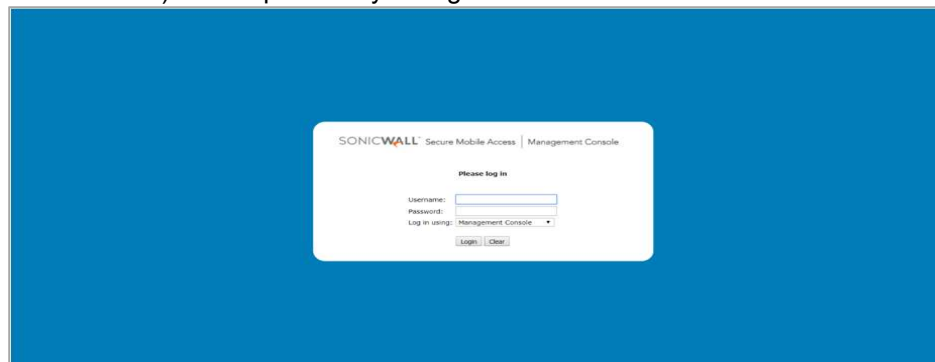


After clicking the 'Finish' button, the changes will be applied.



2.3 Accessing Secure Mobile Access Management Console

Connect to Access Management Console (AMC) with a browser by typing url: "https://<IP address>:8443" (where <IP address> matches the IP address of the internal network interface, by default it is 192.168.0.10). Enter previously configured credentials to authenticate to AMC.



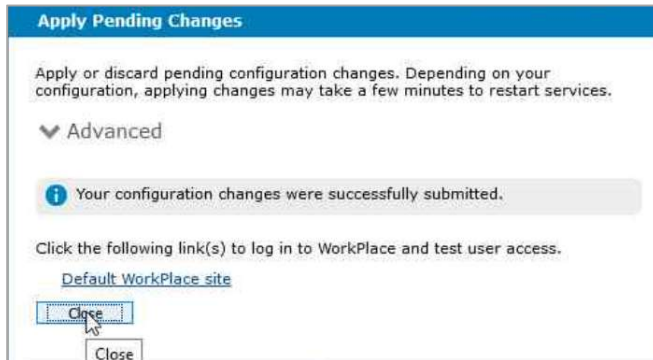
SonicWall SMA v12.1

Once successfully authenticated, the AMC dashboard will be displayed.

To terminate AMC session, click 'Log out' link in the top right corner.

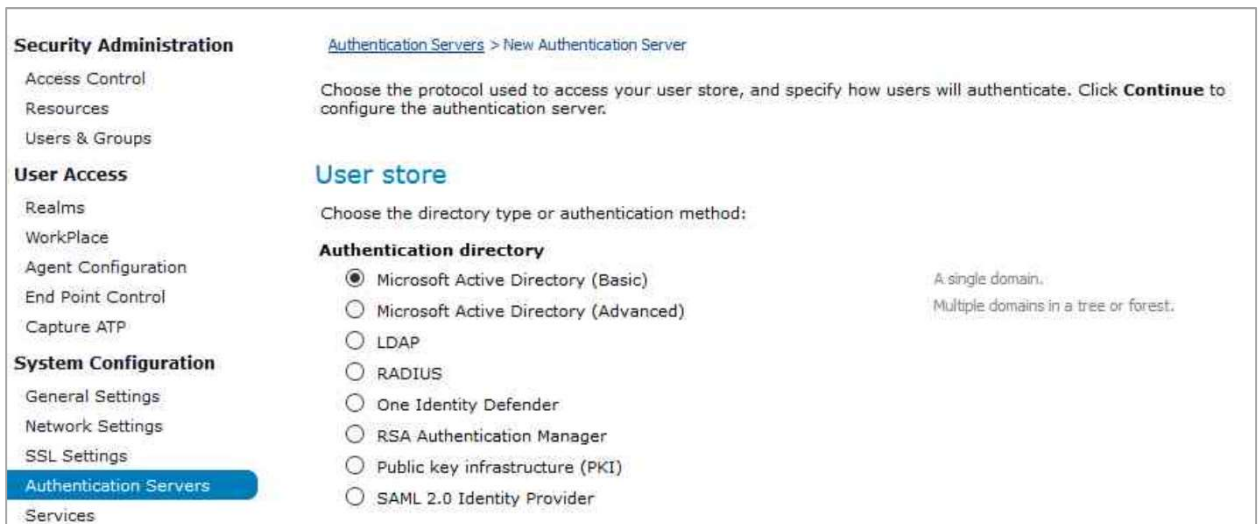
2.4 Evaluated Configuration

Note: Some configuration changes require applying pending changes to take effect.



1. Create a new local authentication server and configure password policy

- Login to AMC using administrative credentials
- Select **System Configuration** → **Authentication Servers**
- Click **New**



- Select **Local users** under Local users storage from the right pane, and leave everything else unchanged



- Click **Continue**
- Type "local-auth" in Name:* field



- Under Password policy checkbox **Lowercase letters**, **Numeric digits (0-9)**, **Uppercases letters**, and **Symbols** check boxes

Password policy

Passwords are to characters in length

Passwords must contain at least one of the following:

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

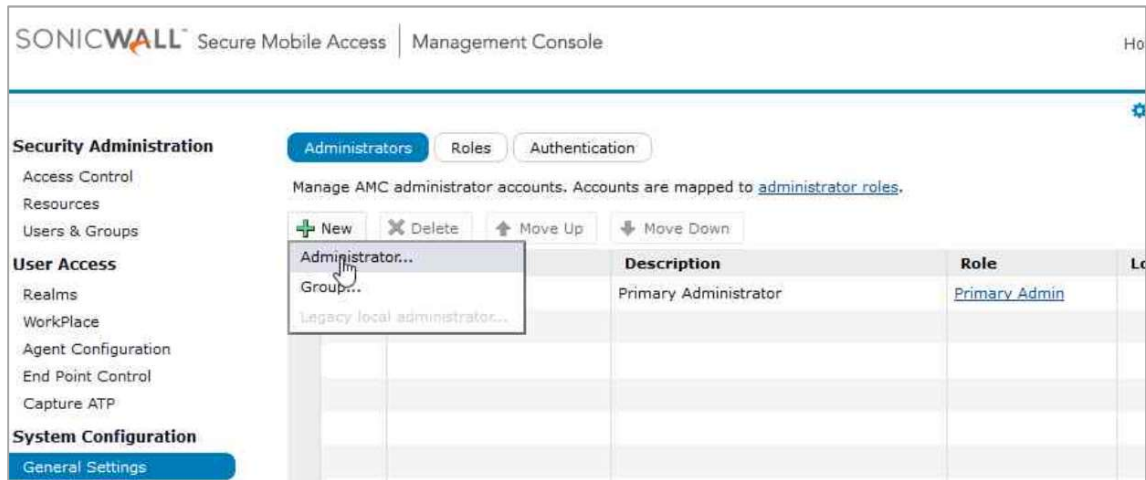
- Click on **Save** button
- Navigate to **System Configuration** → **General Settings**
- Click on **Authentication** button
- Select "local-auth" from the Authentication server: drop-down menu



- Click on **Save** button
- Apply Pending Changes

2. Create a new local administrator

- Select **System Configuration** → **General Settings**
- Click **Administrators**
- Click **New** and select Administrator...



- Populate mandatory fields and click **Save**

[Administrators](#) > Add Administrator

Select a user to assign to an administrator. You must have [configured](#) for Management Console.

User: *

Role:

Manage users and groups stored in the local user repository.

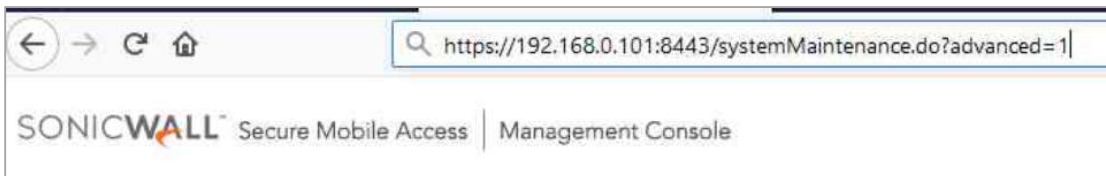
Filters ([reset](#))

Name: Description: Type: Used:

<input type="checkbox"/>	Type	Name ^	Description	Used	Last logged in
<input type="checkbox"/>		ccadmin	Common Criteria Admini...		

3. **Configure Admin account user name and password restrictions, lockout**

- Navigate to **System Configuration** → **Maintenance** page.
- Modify the URL by appending a query parameter `?advanced=1` and hit enter.



- Click on “**Configure...**” button under **Advanced** → **Configuration extension**

The screenshot shows the SonicWall SMA v12.1 web interface. The left sidebar contains a navigation menu with the following items: Agent Configuration, End Point Control, Capture ATP, System Configuration (highlighted in blue), Maintenance, Monitoring, User Sessions, System Status, Logging, and Troubleshooting. The main content area is titled 'System configuration' and is divided into three columns. The first column, 'Import or export', contains the text 'Import configuration data from another system or from backup, or export the current configuration for replication or backup.' and an 'Import/Export...' button. The second column, 'Central Management', contains the text 'Include this appliance in a pool of appliances that is licenced and managed by a central management server.' and a 'Configure...' button. The third column, 'System software updates', is further divided into 'Update' and 'Rollback' sections. The 'Update' section contains the text 'Install a system upgrade or hotfix on the appliance.' and an 'Update...' button. The 'Rollback' section contains the text 'Restore a previous version of the system software or remove a hotfix.' and a 'Rollback...' button. Below these sections is the 'Advanced' section, which includes 'Configuration extensions' and 'Apply All'. The 'Configuration extensions' section contains the text 'Configure extended features and functionality as directed by SonicWall technical support.' and a 'Configure...' button. A tooltip 'Configure Extensions' is visible over the 'Configure...' button. The 'Apply All' section contains the text 'Trigger AMC to push out all configuration files and restart all services the next time pending changes are applied.' and an 'Apply All' button.

- Click on “New” button
- Add a new configuration extension `MGMT_ALLOW_MODIFY_ADMIN` and set its value to `true`
- Add a new configuration extension `DISALLOW_ROOT_ACCESS` and set its value to `true`
- Add a new configuration extension `ADMINISTRATOR_ACCOUNT_LOCKOUT_ATTEMPTS` and set value to the threshold (e.g. set a number of successive unsuccessful authentication attempts to 3)
- Add a new configuration extension `ADMINISTRATOR_ACCOUNT_LOCKOUT_SECONDS` and set value to the lockout period in seconds (e.g. 180 seconds lockout)

Note: When root access is disabled, only Primary Administrator can access CLI.

SonicWall SMA v12.1

Security Administration Maintenance > Configuration Extensions

Access Control
Resources
Users & Groups

User Access
Realms
WorkPlace
Agent Configuration
End Point Control
Capture ATP

System Configuration
General Settings
Network Settings
SSL Settings
Authentication Servers
Services
Maintenance

Monitoring

Making changes to configuration extensions will cause AMC to prompt for confirmation before changes are applied.

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

<input type="checkbox"/>	Key	Value
<input type="checkbox"/>	ACCEPTABLE USE BANNER	ONLY A
<input type="checkbox"/>	AMC SESSION TIMEOUT SECS	900
<input type="checkbox"/>	LOGGING SECURE_SYSLOG	true
<input type="checkbox"/>	MGMT_ALLOW_MODIFY_ADMIN	true
<input type="checkbox"/>	MGMT_STRICT_CERTIFICATE_VALIDATION	true

Configuration

- Click on "ok"
- Click on "save" button
- Navigate to **System Configuration** → **General Settings**
- Under Administrators Click **Edit**

Administrators

Administrator accounts

Primary Admin: admin

Edit

Note: Primary Admin username and password can be used to access CLI. In cases when access to AMC is temporarily disabled, CLI can be used to perform a subset of administrative functions.

- Modify `username` field with a custom username
- Click on "save" button

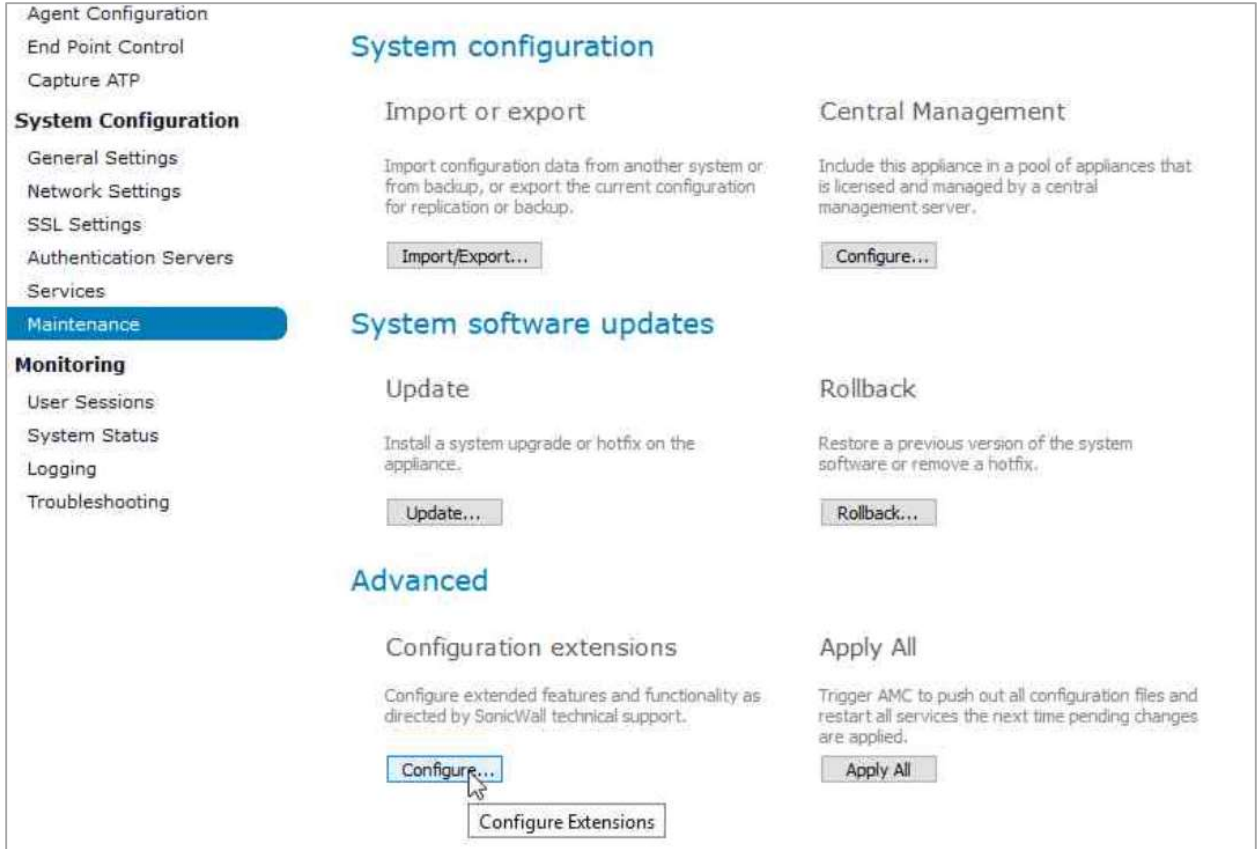
4. Configure idle timeout

- Navigate to **System Configuration** → **Maintenance page**.
- Modify the URL by appending a query parameter `?advanced=1` and hit enter.

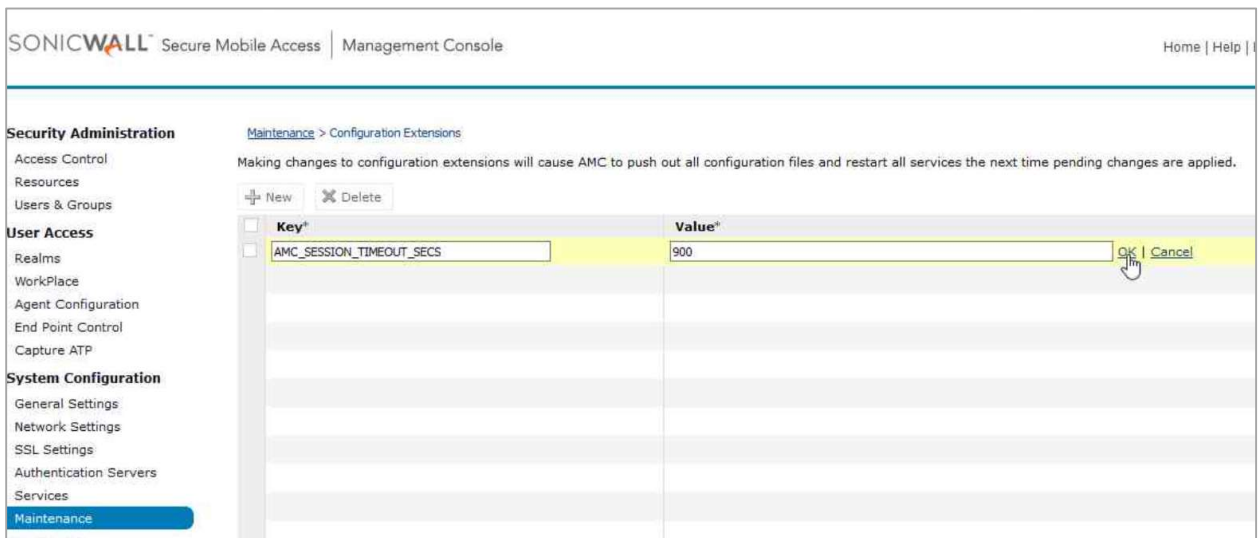
← → ↻ 🏠 🔍 https://192.168.0.101:8443/systemMaintenance.do?advanced=1

SONICWALL Secure Mobile Access | Management Console

- Click on "Configure..." button under **Advanced** → **Configuration extension**



- Click on “New” button
- Add a new parameter **AMC_SESSION_TIMEOUT_SECS** and set idle timeout in seconds.
Ex: Set Key= AMC_SESSION_TIMEOUT_SECS and value=900
- Click on “ok” link



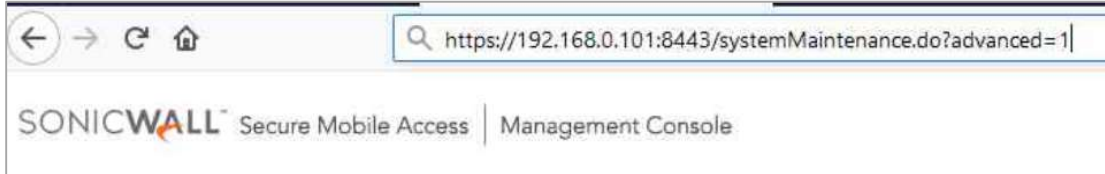
- Click on “save” button.

SonicWall SMA v12.1

- **Apply** All pending changes

5. Configure Login Banner

- Navigate to **System Configuration** -> **Maintenance** page.
- Modify the URL by appending a query parameter `?advanced=1` and hit enter.



- Click on "Configure..." button under **Advanced/Configuration extensions**.
- Click on "New" button.
- Add a new parameter "ACCEPTABLE_USE_BANNER" and set value to the message you wish to display as banner during authentication
Ex: Set Key= ACCEPTABLE_USE_BANNER and value=Welcome User! You are logging in
- Click on "Ok" link.
- Click on "Save" button
- Apply Pending Changes

6. Disable Services that are not required part of the evaluated configuration

- Navigate to **System Configuration** → **Services**
- Check the following services are **disabled** by default, else click **Configure** → **Select** → **Disable**
<service name>
 - **SNMP**
 - **SMTP**
 - **SSH**

SSH

Use Secure Shell (SSH) to safely access the appliance command line from another host.

[Configure](#)

Status: **Disabled**

SNMP

Monitor the appliance from a Simple Network Management Protocol (SNMP) management tool.

[Configure](#)

Status: **Disabled**

SMTP

Allow the appliance to send email using a Simple Mail Transfer Protocol (SMTP) mail server.

[Configure](#)

Status: **Disabled**

7. Enable FIPS mode

Warning: Enabling FIPS mode will delete existing keys and certificates.

- Navigate to **System Configuration** → **General Settings**
- Click on “**Edit**” link under FIPS security.
- Enable FIPS mode and click on “**Save**” button.



- Apply Pending Changes and wait for reboot

8. Configure trusted Certificate Authorities (CAs)

Note: If OCSP signing is delegated to a different CA, such CA certificate also must be explicitly trusted and configured as a designated responder.

- Navigate to **System Configuration** → **SSL Settings**
- Select CA Certificates → **Edit**
- Select **New**
- Click **Browse** under Import CA Certificate



- Enable the following for the usage:
 - **Web Server connections (HTTPS)**
 - **OCSP response verification**

Note: Other Usage may be applicable depending on the specific deployment.

- Click **Import**

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.

9. Configure SMA web server certificate

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

- Navigate to **System Configuration** → **SSL Settings**
- Next to **SSL Certificates** click **Edit** link

SonicWall SMA v12.1

The screenshot shows the SonicWall SMA v12.1 Management Console. The top navigation bar includes the SonicWall logo, "Secure Mobile Access", and "Management Console". On the left, a sidebar menu lists categories: "Security Administration" (with sub-items: Access Control, Resources, Users & Groups), "User Access" (with sub-items: Realms, WorkPlace, Agent Configuration, End Point Control, Capture ATP), and "System Configuration" (with sub-items: General Settings, Network Settings, and SSL Settings, which is highlighted). The main content area is titled "SSL certificates" and contains three sections: "Default appliance certificate (WorkPlace and other access methods)" with a value of "N/A" and an "Edit" button; "Management console certificate (AMC)" with a value of "192.168.0.101 (self-signed)" and a validity period of "Valid through: 01 Jan 2022"; and "Virtual hosting certificates for WorkPlace sites and URL resources" with a value of "192.168.0.101". Below these sections is a "CA certificates" section with a red warning icon and the text: "One or more CA certificates in use have expired, which may prevent users from authenticating." A callout box labeled "SSL Certificates" points to the "Edit" button.

- Click **Certificate Signing Request**

The screenshot shows the SonicWall SMA v12.1 Management Console with the "SSL Settings > SSL Certificates" breadcrumb. The left sidebar menu is the same as in the previous screenshot. The main content area is titled "Certificates" and has two tabs: "General" and "Certificate signing requests", with the latter being selected. Below the tabs, the text "Manage SSL server certificates used to" is followed by a dropdown menu currently showing "Certificate signing requests". A callout box labeled "Certificate signing requests" points to the dropdown menu.

- Click **New**
- Populate certificate information field, ensuring that `Alternative names` field that corresponds to SAN extension contains a unique identifier in form of FQDN or IPv4 address.

Certificate information

The information below will be stored in the CSR and used in your SSL certificate.

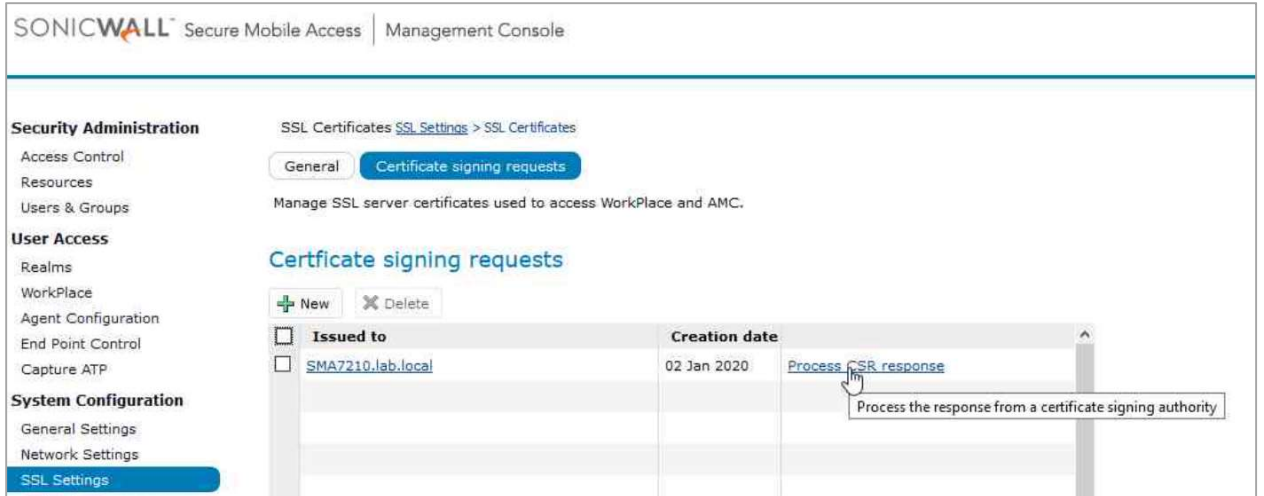
Fully qualified domain name: *	<input type="text"/>	This name will appear in the certificate. It will be visible to users, and must be added to your DNS.
Alternative names:	<input type="text"/> Create Certificate Signing Request	Enter any additional FQDNs (or IP addresses) that will appear in the certificate using the Subject Alternative Name certificate extension.
Organizational unit:	<input type="text"/>	Your division or department. For example, MIS Dept.
Organization: *	<input type="text"/>	For example, ABC Corporation. Most commercial CAs require you to enter this exactly as it appears on your articles of incorporation.
Locality:	<input type="text"/>	For example, Seattle. No abbreviations.
State: *	<input type="text"/>	No abbreviations.
Country: *	<input type="text"/>	Two-letter abbreviation only, for example, US or AU.
Key type:	Key size:	Signature:
<input type="text" value="RSA"/>	<input type="text" value="2048 bits"/>	<input type="text" value="SHA-384"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

- Click **Save**
- Securely transfer the new certificate request to the trusted Certificate Authority for signing

Note: Certificate Signing request includes ---- BEGIN and ----- END lines and is typically a .csr or .pem binary file.

- Receive signed certificate back from a trusted CA
- Navigate to **System Configuration** → **SSL Settings**
- Select **SSL Certificates** → **Edit**
- Click **Certificate Signing Request**
- Click **Process CSR Response** link next to the newly created CSR

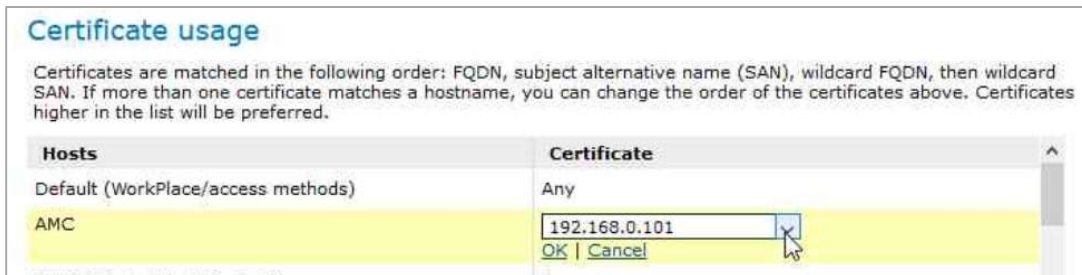
SonicWall SMA v12.1



- Securely upload the signed certificate request

Note: Signed certificate includes ---- BEGIN CERTIFICATE and ----- END CERTIFICATE lines and is typically a .pem binary file.

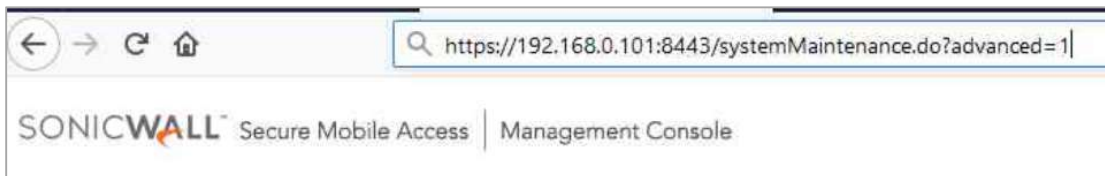
- Click **Save**
- Under **Certificate usage** next to **AMC** confirm that the new certificate is selected



- Apply Pending Changes

10. Configure TLS settings

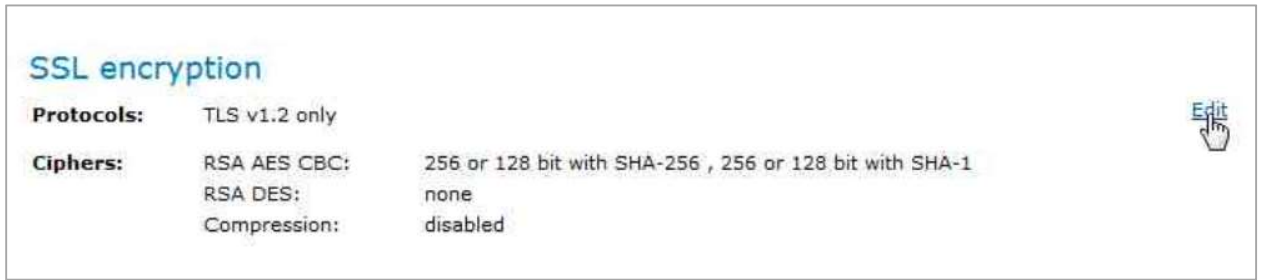
- Navigate to **System Configuration -> Maintenance** page.
- Modify the URL by appending a query parameter **?advanced=1** and hit enter.



- Click on "Configure..." button under **Advanced/Configuration extensions**.
- Click on "New" button.
- Add a new parameter **MGMT_STRICT_CERTIFICATE_VALIDATION** and set value to "true"
- Click on "Ok" link.
- Click on "Save" button
- Apply Pending Changes

SonicWall SMA v12.1

- Navigate to **System Configuration** → **SSL Settings**
- Click on “**Edit**” link next to SSL Encryption



- Select “**TLS version 1.2 or 1.1**” under SSL protocols

SONICWALL Secure Mobile Access Management Console

Security Administration | [SSL Settings > Configure SSL Encryption](#)

Configure the protocols and compression settings used to encrypt traffic.

Use only US government-recommended encryption Uses FIPS 140-2 compliant encryption settings. FIPS is a government standard specifying best practices for implementing cryptographic software.

SSL protocols

Select the protocols that are accepted by the access servers.

TLS version 1.2 only 'Any TLS version' includes TLS 1.0, 1.1, and 1.2.

TLS version 1.2 or 1.1

Any TLS version ⚠

SSL ciphers

Select the SSL ciphers you want connecting clients to use. Ciphers are attempted in the order listed. If a client is unable to use any selected ciphers, they will not be able to connect to the appliance.

[Reset to defaults](#)

Enabled	Cipher	Performance	Strength	Order
<input checked="" type="checkbox"/>	RSA AES 128-bit CBC with SHA-1 ⓘ	++++	+++	▼
<input checked="" type="checkbox"/>	RSA AES 256-bit CBC with SHA-1 ⓘ	***	****	▲▼
<input checked="" type="checkbox"/>	RSA AES 128-bit CBC with SHA-256	++	++++	▲▼
<input checked="" type="checkbox"/>	RSA AES 256-bit CBC with SHA-256	**	****	▲▼

- Select the following TLS ciphers to be used under “**SSL ciphers**”:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256

- Click on “**save**” button.
- Apply Pending Changes

11. Configure audit policy

- Navigate to **Monitoring** → **Logging**
- Click **Configure Logging** → **Services Log Level**

Level	Time	Username
Info	1/2/20 16:25:42	ccadmin
Info	1/2/20 16:24:46	ccadmin
Info	1/2/20 16:24:06	ccadmin
Info	1/2/20 16:23:51	ccadmin
Info	1/2/20 16:22:24	ccadmin
Info	1/2/20 16:20:15	ccadmin
Info	1/2/20 16:19:51	ccadmin
Info	1/2/20 16:16:52	ccadmin
Info	1/2/20 16:08:03	ccadmin
Info	1/2/20 15:52:47	ccadmin

- Under Service log level ensure that Web Proxy and Network tunnel log levels are set to Info

Services log level

Choose the log levels for the various services.

Web proxy: Info Network tunnel: Info Management: Debug

Collect system health information

- Under Service log level configure Management log level to Debug
- Click **Save**

12. Configure external audit server (syslog)

- Navigate to **System Configuration** -> **Maintenance** page.
- Modify the URL by appending a query parameter **?advanced=1** and hit enter.

SonicWall SMA v12.1

- Click on “Configure...” button under **Advanced/Configuration extensions**.
- Click on “New” button.
- Add a new parameter **LOGGING_SECURE_SYSLOG** and set value to “true”
- Click on “Ok” link
- Click **Save**
- Navigate to **Monitoring → Logging**
- Under Syslog Configuration **add IP Address and Port number of a Syslog Server**
- Select Protocol: **TCP**

Syslog configuration

Choose one or more syslog servers to which all log information is sent. Regardless of these settings, all events are logged locally. The port number is optional and will default to 514 if left blank.

Server #1:	<input type="text" value="192.168.0.204"/>	Port: <input type="text" value="6514"/>	Protocol: <input type="text" value="TCP"/>
Server #2:	<input type="text"/>	Port: <input type="text"/>	Protocol: <input type="text" value="TCP"/>
Server #3:	<input type="text"/>	Port: <input type="text"/>	Protocol: <input type="text" value="TCP"/>

- Click **Save**
- Apply Pending Changes

3 Auditable Events

To access audit records through AMC, navigate to **Monitoring** → **Logging** → **View Logs**

View system logs and configure the log settings.

Log file: Management audit log (selected) Show last: 1000 messages Auto-refresh: 1 min. Refresh

Level: Error Warning Info Verbose Export...

Level	Date and Time	Username	Message
Info	1/10/20 15:02:08	ccadmin	Login succeeded - Address=192.168.0.162
Info	1/10/20 15:02:08	ccadmin	Logout - Address=192.168.0.162 Duration=00:00:00 Expired=true
Info	1/10/20 14:36:45	ccadmin	Login succeeded - Address=192.168.0.162
Info	1/10/20 14:36:45	ccadmin	Logout - Address=192.168.0.162 Duration=00:15:23 Expired=true
Info	1/10/20 14:21:21	ccadmin	Login succeeded - Address=192.168.0.162
Info	1/10/20 13:38:14	ccadmin	Logout - Address=192.168.0.162 Duration=01:00:35 Expired=true
Info	1/10/20 13:07:43	ccadmin	Login succeeded - Address=192.168.0.162
Info	1/10/20 12:37:38	ccadmin	Logout - Address=192.168.0.162 Duration=00:00:37 Expired=false
Info	1/10/20 12:37:26	admin	Applied configuration changes
Info	1/10/20 12:37:23	admin	Updated administrator account - ID=PrimaryAdmin Username=ccadmin Role=Primary Admin Password changed=false
Info	1/10/20 12:37:15	admin	Updated administrator account - ID=PrimaryAdmin Username=ccadmin Role=Primary Admin Password changed=false

Each audit record contains the following information: type of event, date and time of the event, subject identity, and the outcome.

Type	Date and Time	Identity	Outcome
Info	1/10/20 12:37:38	ccadmin	Login succeeded - Address=192.168.0.162

SonicWall SMA v12.1

The SMA supports six levels of audit events: Fatal, Error, Warning, Info, Verbose, and Debug. For each audited event, the date and time, the type of event, the subject identity (e.g. IP address or user identity), and the outcome are logged. The audit records may also contain event-specific content.

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

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

SonicWall SMA v12.1

Auditable Actions	Audit Records
Configure password complexity	<p>Info 8/27/19 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>
TLS configuration	<p>Info 8/2/19 16:44:01 admin Deleted SSL protocol - Name=TLSv1 Info 8/2/19 16:41:52 admin Added SSL protocol - Name=TLSv1_2</p> <p>Info 8/2/19 16:45:46 admin Deleted SSL cipher - Name=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</p> <p>Info 8/2/19 16:45:46 admin Changed order of SSL cipher - Name=TLS_RSA_WITH_AES_256_GCM_SHA384 From=2 To=0</p>
FIPS mode	<p>Info 6/20/19 13:21:25 admin Updated FIPS settings - Enabled=true Info 6/20/19 13:35:46 admin Updated FIPS settings - Enabled=false</p>
Audit server configuration	<p>Info 8/2/19 16:53:59 admin Updated syslog settings: Server1=10.5.252.101:9999/tcp Server2=None Server3=None</p>

SonicWall SMA v12.1

Auditable Actions	Audit Records
<p>X.509 Certificate management</p> <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).</p> <p>Certificate Signing Request (CSR) An entity that wants a signed certificate or a digital certificate requests one through a CSR.</p>	<p><u>Certificate Authority (CA)</u></p> <p>Info 8/8/19 09:25:19 admin Added CA certificate - Issued to=ROOTCA Info 8/8/19 09:25:04 admin Deleted CA certificate - Issued to=ROOTCA</p> <p><u>Certificate Signing Request (CSR)</u></p> <p>Info 6/12/19 15:40:13 admin Added SSL certificate signing request - Issued to=example.sonicwall.com Info 8/8/19 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 Error 6/26/27 11:35:39 AMC unable to import CSR reply:java.io.IOException: Incomplete BER/DER data</p>
<p>Verifying and applying updates</p>	<p><u>Uploading a Valid hotfix file:</u></p> <p>Info 6/24/19 10:47:57 admin Installed hotfix pform-hotfix-12.1.0-06163</p> <p><u>Uploading an Invalid hotfix file:</u></p> <p>Error 8/2/19 17:36:15 admin Hotfix update failed: Hotfix file integrity check failed.</p>
<p>Configuring system time</p>	<p>Info 6/12/19 12:59:17 admin Set time to Wed Jun 12 12:59:17 IST 2019</p>
<p>Configuring and modifying access banner</p>	<p>Info 8/2/19 17:57:08 admin Added configuration extension - Key=ACCEPTABLE_USE_BANNER Value=Welcome to AMC</p>
<p>Configuring termination of interactive remote session</p>	<p>Info 8/2/19 18:05:18 admin Added configuration extension - Key=AMC_SESSION_TIMEOUT_SECS Value=30</p>

SonicWall SMA v12.1

Auditable Actions	Audit Records
Operations related to cryptographic keys or certificates	<p>Commands to delete TOE's identity (i.e. web) certificate:</p> <p>Info 8/5/19 09:21:01 admin Added SSL certificate - Issued to=192.168.0.10 Info 8/5/19 09:21:07 admin Updated SSL certificate - Usage=AMC Issued to=192.168.0.10 Info 8/5/19 10:02:36 admin Deleted SSL certificate - Issued to=172.29.0.204</p> <p>Commands to delete trusted CA:</p> <p>Info 8/5/19 10:08:07 admin Deleted CA certificate - Issued to=Unit Testing CA</p>

SonicWall SMA v12.1

Auditable Actions	Audit Records
<p>Administrative login</p>	<p><u>Successful administrative login:</u></p> <p>Info 6/11/19 09:00:14 admin Login succeeded - Address=10.1.101.10</p> <p><u>Unsuccessful administrative login:</u></p> <p>Warning 6/11/19 06:26:28 AMC Authentication failed: Username=admin, Address=10.1.101.10</p> <p><u>Unsuccessful login attempt limit is met or exceeded:</u></p> <p>Info 7/25/19 14:52:50 admin Added configuration extension - Key=ADMINISTRATOR_ACCOUNT_LOCKOUT_SECONDS Value=180 Info 7/25/19 14:52:50 admin Added configuration extension - Key=ADMINISTRATOR_ACCOUNT_LOCKOUT_ATTEMPTS Value=4 Error 8/5/19 11:58:13 admin Administrator account locked due to 3 successive login failures</p> <p><u>Timeout of local administrative session:</u></p> <p>Sep 3 15:55:04 SMAAppliance -bash: Timeout, session closed for user(root) Sep 3 15:55:04 SMAAppliance login[4754]: pam_unix(login:session): session closed for user root</p> <p><u>Timeout of remote administrative session:</u></p> <p>Logout - Address=192.168.56.1 Duration=03:15:57 Expired=true</p> <p><u>Administrator logging off:</u></p> <p>Info 6/21/19 13:24:57 admin Logout - Address=10.5.22.125 Duration=00:00:26 Expired=false</p>

SonicWall SMA v12.1

Auditable Actions	Audit Records
<p>Account management</p>	<p><u>Creation of a new user:</u></p> <p>Info 6/24/19 19:32:12 admin Added administrator account - Username=user1</p> <p><u>Disabling of user account by administrative action:</u></p> <p>Info 8/26/19 12:26:15 admin Updated local user - ID=AV1565098985406CPP Name=user1 Password changed=false Enabled=false</p> <p><u>Deletion of existing account:</u></p> <p>Info 6/24/19 20:12:34 admin Deleted administrator account - ID=AV1561384932759GQT Username=user1</p> <p><u>Reset of User Password:</u></p> <p>Info 8/6/19 19:07:46 admin Updated administrator account - ID=PrimaryAdmin Username=admin Role=Primary Admin Password changed=true</p>
<p>Failure to establish a TLS session</p>	<p>Error 6/24/19 15:41:31 AMC SSL handshake failed: Client requested protocol TLSv1 not enabled or not supported.</p> <p>Error 6/25/19 15:26:35 AMC SSL handshake failed: no cipher suites in common</p>

SonicWall SMA v12.1

Auditable Actions	Audit Records
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=sma1000/CN=ROOT', hostname='10.1.111.101', certificate='ROOT'