SonicWall® Secure Mobile Access 12.1

Upgrade Guide

October 2017, updated February 2018

This document describes the process of updating your SonicWall® Secure Mobile Access (SMA) firmware. Specific upgrade scenarios include:

- Upgrading a standalone SMA 1000 appliance
- Upgrading the Central Management Server (CMS) along with its managed SMA 1000 appliances

Topics:

- Upgrade Description
- Special Considerations
- Preparation
- SMA Infrastructure Upgrade
- Post-Upgrade Tasks

Upgrade Description

Upgrading your SMA infrastructure is a multi-task process that includes obtaining the updates or hotfixes, updating the SMA appliances, and updating the client endpoints. Instructions for creating a MySonicWall account and how to register your appliances are also included, if you haven't already done that.

Topics:

- Upgrade Summary
- Platform Compatibility
- Deprecated Features

Upgrade Summary

To upgrade process for Secure Mobile Access includes updating both the SMA appliances and the client end points, such as a user's laptop. Instructions for both are provided. The following lists summarizes the general process for an upgrade.

1 Create a MySonicWall account, if you don't already have one. MySonicWall is a resource center, giving you access to many tools and support.

> **NOTE:** MySonicWall registration information is not sold or shared with any other company.

2 Register your devices on MySonicWall. Registration provides access to essential resources, such as your license file, firmware updates, documentation, and technical support information.

3 Retrieve the update file for your Secure Mobile Access appliance and for the client end points from MySonicWall.

4 Upload and install the update file:

- For standalone appliances: upload and install the update file using the Appliance Management Console (AMC).
- For CMS managed appliances: upload and install the update file using the Central Management Console (CMC).

5 Upload and install the update file to your appliance using the Appliance Management Console (AMC).

> ⓘ **NOTE:** The appliance is rebooted as a part of the upgrade process.

6 Install the client upgrade on all the client endpoint upgrade and verify them.

Platform Compatibility

The SMA 12.1 Central Management Service with Global Traffic Optimizer supports the following SMA 1000 series appliances running SMA 12.1 firmware:

- EX9000
- EX7000
- EX6000
- SMA 6200
- SMA 7200
- SMA 8200v (ESX/Hyper-V)

You can upgrade a Secure Mobile Access appliance directly to version 12.1 from versions 10.7.2, 11.3.0, and 11.4.0.

> ⓘ **NOTE:** Upgrading a virtual appliance hosted on ESXI requires network adapter changes. Refer to the SonicWall Support Knowledge Base article at: https://www.sonicwall.com/support/knowledge-base/170502800288963.

Deprecated Features

The following features have been deprecated on all SMA 1000 series appliances in SMA 12.1:

- **Global Management System (GMS)**

  GMS is not supported in SMA 12.1, but it does not need to be manually disabled. SMA 12 devices must be managed by the Central Management Service with Global Traffic Optimizer. Please refer to the *SMA 12.1 Central Managment Server with Global Traffic Optimizer Administration Guide* for details.

- **Secure Sockets Layer (SSL) Version 3.0**

  The system automatically disables SSLv3 when upgrading to SMA 12.1 or when importing the configuration. This applies to standalone appliances and CMS installations. The SSLv3 protocol is not supported or negotiated for any connections in SMA 12.1 During system upgrade or configuration import, if SSLv3 is enabled on the incoming configuration, it is removed from the new configuration and the upgrade or import process succeeds.

- **Virtual Assist**

  When you attempt to upgrade to SMA 12.1 from an earlier release or import an SMA 12.1 configuration, the system prevents the upgrade or import and notifies you with the following message:

  ```
  Virtual Assist is not available in SMA 12.1. You must disable
  Virtual Assist before you can upgrade to SMA 12.1.
  ```

  You can disable Virtual Assist on the **System Configuration > Virtual Assist > General** page, and then start the upgrade process again. Once Virtual Assist is disabled, the upgrade process completes successfully.

- **Replication**

  CMS provides Global High Availability (GHA), which provides redundancy. Therefore, the Replication feature has been removed from SMA, and all references to the replication feature have been removed from the Appliance Management Console. The **Replicate** section no longer appears on the **Maintenance** page, and the entire **Configure Replication** page, accessed via the **Configure** button, has been removed. In SMA 12.1, CMS Policy Synchronization is the equivalent of the old Replication feature.

- **High Availability Pair**

  High Availability (HA) Pair has been deprecated. The Central Management Service with Global Traffic Optimizer replaces HA Pair. The CMS and Central User licenses replace HA Pair licenses.

  All HA Pair connections must be disabled before you can upgrade to SMA 12.1. Attempting to upgrade a node in an HA Pair to SMA 12.1 does not succeed and generates this error message:

  ```
  Except: Special CEM to allow upgrade that breaks node out of pair.
  ```

- **Virtual Host with IP Address**

  Upgrading to SMA 12.1 may not succeed if any virtual hosts with IP addresses are defined in the current configuration. Importing the full SMA 12.1 configuration does not succeed, but importing a partial SMA 12.1 configuration succeeds if the extra IP addresses are removed from the current configuration first.

Special Considerations

Some customer configurations may need some additional consideration when planning your SMA upgrade. Since HA Pairs have been deprecated, you need to reconfigure your appliances to break up the pair. Solutions with Connect Tunnel implemented also has special considerations for updating endpoints.

Topics:

- Upgrading HA Pairs
- Connect Tunnel Upgrade Requirements
- Upgrading OSPWAT OESIS libraries from V3 to V4

Upgrading HA Pairs

The Central Management Service with Global Traffic Optimizer makes the HA Pairs obsolete. Once upgraded, traffic can be distributed across the appliances seamlessly, and an appliance failure has limited affect on the user. To take advantage of this new features, be aware of the following items as you upgrade:

- Central Management Service with Global Traffic Optimizer requires Central User Licenses to ensure Global High Availability among your appliances. You can exchange your HA Pair licenses for Central User Licenses. Support licenses are no longer needed.
- If you have appliances that are nodes in a High Availability (HA) Pair, you cannot upgrade them directly to SMA 12. The upgrade process recognizes that it is being run on a node in an HA Pair and blocks the upgrade process. You need to disable the HA Pair before you can continue.
- If you configure an extension mechanism (or CEM) to acknowledge that the upgrade results in a standalone appliance, the upgrade is allowed to continue. The upgrade assumes the identity (name/addresses) of the node being upgraded. After upgrading, the two new stand alone appliances may share overlapping resources between them. For example, the address pools for each appliance are identical. Running the upgrade process with the CEM results in two standalone appliances running SMA 12.1.
- Currently, a full import of the configuration is not allowed from an HA appliance onto a standalone appliance. You can import a partial configuration from an HA appliance onto a standalone appliance, as well as onto a CMS.

Connect Tunnel Upgrade Requirements

Client component upgrades follow the same requirements as appliance upgrades. Hotfixes on the client should be up to date before the upgrade.

You can upgrade appliance and client components to 12.1 as shown below:

- 12.0.1 + Latest Hotfixes -> 12.1
- 10.7.2 + Latest Hotfixes -> 12.1
- 11.3.0 + Latest Hotfixes -> 12.1
- 11.4.0 + Latest Hotfixes -> 12.1

ⓘ **IMPORTANT:** Upgrading from 10.7.2 and 11.3.0 are not supported for Connect Tunnel client connections or for upgrades in a GTO domain. You should upgrade to the GTO version 11.4.0 first and then upgrade to 12.1.

After you download the client hotfix to your appliance, the client-side fixes are then automatically pushed to each client system as it connects to the appliance. Depending on your environment, this can take a few days, weeks, or even months before all clients have connected and received the client-side fixes.

ⓘ **NOTE:** To use Central Management Service with Global Traffic Optimizer, Connect Tunnel clients must upgrade to SMA 11.4 or higher.

Upgrading OSPWAT OESIS libraries from V3 to V4

The OESIS V3 libraries have already been declared out of support by OPSWAT. However, for existing customers like SonicWall, OPSWAT will continue supporting them for a period of time.

Refer to this Knowledge Base article for more information:
https://www.sonicwall.com/support/knowledge-base/171004181702551.

Preparation

You need to complete several tasks before updating your SMA infrastructure:

- Finding the Authentication Code
- Creating a MySonicWall Account
- Registering your SMA Appliance
- Obtaining the Update File or Hotfix
- Verifying the Downloaded Update File
- Backing up your Current Configuration

Finding the Authentication Code

When you register your SMA appliance, you need to provide an authentication code. Your authentication code is the hardware identifier for your appliance. It is displayed in the following places:

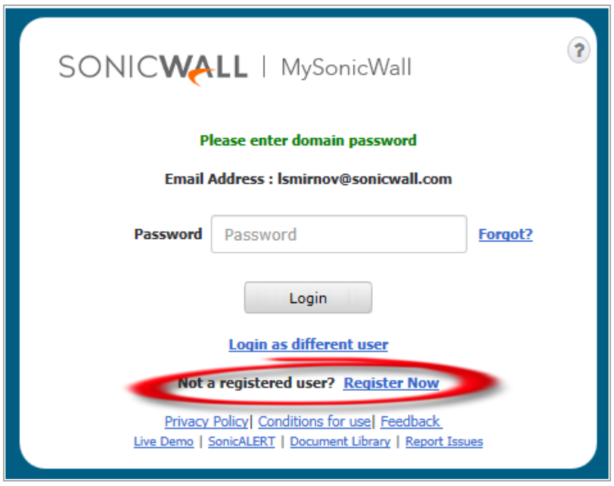
- On the appliance label
- On the **General Settings** page in the Appliance Management Center

Creating a MySonicWall Account

MySonicWall is a resource center designed specifically for SonicWall customers. Through it, you have access to current security notices, updates and hotfixes, support, training, and documentation. You can also use MySonicWall to register your products and manage your licenses. If you do not already have a MySonicWall account, create one by completing an online registration.

To create a MySonicWall account:

1 In your Web browser, navigate to https://www.mysonicwall.com/.


SONICWALL | MySonicWall
?

Please enter domain password

Email Address : lsmirnov@sonicwall.com

Password: Password

Forgot?
Login
Login as different user
Not a registered user? Register Now
Privacy Policy| Conditions for use| Feedback
Live Demo | SonicALERT | Document Library | Report Issues

2 Click on **Register Now**.

3 Enter your account information, personal information, and preferences, and then click **Register**. Be sure to use a valid email address.

4 Follow the prompts to finish creating your account. SonicWall sends a subscription code to the email address you entered in Step 3.

5 When you return to the login screen, log in with your new username and password.

6 Confirm your account by entering the subscription code you received by email.

Registering your SMA Appliance

Registering your appliances ensures that you have access to the latest updates and hotfixes.

To register your appliance:

1 Locate your software serial number, which is printed on the back of your SonicWall appliance.

2 Navigate to MySonicWall and log in with your username and password.

3 In the Quick Register section, enter your serial number, and then click **Next**.

4 Follow the on-screen instructions from the wizard, which includes providing the authentication code.

5 Confirm your serial number.

6 Enter a name for this appliance.

7 Click **Register** to continue.

8 Follow the online prompts to finish the survey and complete the registration process.

Obtaining the Update File or Hotfix

To obtain the update file:

1 Navigate to https://www.mysonicwall.com/ in the browser of your choice.

2 Log in with your username and password.

3 On the **Downloads > Download Center** page, select your appliance model from the **Software Type** drop-down list.

4 In the **Available Software** list, select the update file or hotfix that corresponds to your appliance.

For a new firmware version, you’re prompted to download a file named *<part number>_upgrade-<n>_<n>_<n>_<three-digit build number>.bin* file to your local computer. Hotfix filenames use the following naming convention: *<component>-hotfix-<version>-<hotfix number>.bin*.

ⓘ **NOTE:** You can download the upgrade for the client endpoints while still logged into MySonicWall.

Verifying the Downloaded Update File

To verify that the update was successfully transferred to your local computer, compare its checksum against the MD5 checksum information displayed on MySonicWall.

To verify the MD5 checksum of the upgrade file on a PC, use a Windows- or Java-based utility. Microsoft, for example, offers an unsupported command-line utility on their site named *File Checksum Integrity Verifier (FCIV).* Follow these steps to compare checksums using this utility:

1 At the DOS command prompt, type the following, which returns a checksum for the downloaded file:

```
fciv <upgrade_filename>.bin
```

2 Compare the result against the MD5 checksum displayed on MySonicWall. If they match, you can safely continue with your update. If they differ, try the download again and compare the resulting checksums. If they still do not match, contact Technical Support.

3 To verify the MD5 checksum directly on your appliance, type the following command to see the checksum for the downloaded file:

```
md5sum <upgrade_filename>.bin
```

Backing up your Current Configuration

Before updating, back up the current configuration of your appliance. You can use the export feature in the Appliance Management Console (AMC). These steps are optional, but recommended.

1 From the main AMC navigation menu, select **Maintenance**.

2 In the **System Configuration** area, click **Import/Export**.

3 Click the **Export** button.

4 When it prompts you to open the `.aea` file or save it, save it to your hard drive.

ⓘ **NOTE:** On Windows operating systems, Internet Explorer may block the download of the .aea file. To work around this, click the information bar that appears beneath the Internet Explorer **Address** box, and then click **Download File**.

SMA Infrastructure Upgrade

Before upgrading, you need to validate the your appliances are running the latest hotfix before upgrading. The most recent Hotfix list for each firmware version as of the release of this document is shown below. Additional hotfixes may be released in the future; access the corresponding Knowledge Base link to see the most up-to-date hotfix recommendations.

Current Hotfixes (as of Publication Date)

Firmware Version	Latest Plaform (Appliance) Hotfix	Latest Client Hotfix	Knowledgebase Article
12.0.1	pform-hotfix-12.0.1-119	clt-hotfix-12.0.1-119	https://www.sonicwall.com/support/knowledge-base/170713184706508
11.4.0	pform-hotfix-11.4.0.-686	clt-hotfix-11.4.0-686	https://www.sonicwall.com/support/knowledge-base/170502420247167

Current Hotfixes (as of Publication Date)

Firmware Version	Latest Plaform (Appliance) Hotfix	Latest Client Hotfix	Knowledgebase Article
11.3.0	pform-hotfix-11.3.0-457	clt-hotfix-11.3.0-457	https://www.sonicwall.com/support/knowledge-base/170502582817541
10.7.2	pform-hotfix-10.7.2-659	clt-hotfix-10.7.2-659	https://www.sonicwall.com/support/knowledge-base/170502660825431

ⓘ **NOTE:** Upgrading a virtual appliance hosted on ESXI is known to have problems. Refer to the SonicWall Knowledge Base article at https://www.sonicwall.com/support/knowledge-base/170502800288963 for more information.

Topics:

- Installing an Update or Hotfix on an Appliance Using AMC
- Upgrading Managed Appliances Using CMS
- Verifying the Update

Installing an Update or Hotfix on an Appliance Using AMC

If you have not already downloaded the update or hotfix file go to Obtaining the Update File or Hotfix for instructions. Save the file to your local system.

ⓘ **NOTE:** The upgrade fails if Virtual Assist/Replication/GMS is enabled.

To install the update or hotfix:

1. From the main navigation menu in AMC, choose **Maintenance**.
2. In the **System software updates** area, select **Update**.
3. Click **Browse** to locate the update or hotfix file, or type the file path.
4. Click **Install Update**. This step may take several minutes, depending on the network connection speed.

   After the file upload process is complete, the update or hotfix is automatically installed on the appliance. You cannot cancel this part of the installation process. The appliance automatically restarts when the installation is complete.

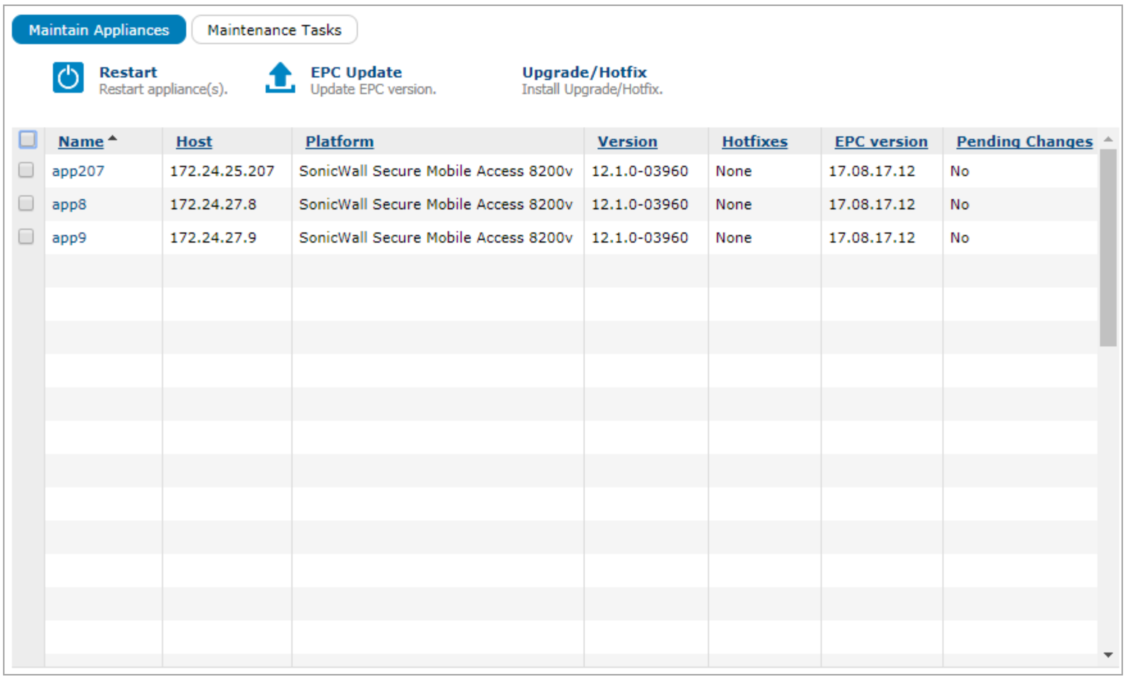
Upgrading Managed Appliances Using CMS

You can use the Central Management console to upgrade and apply hotfixes to your entire VPN infrastructure, including the CMS and all its managed appliances. You can download the CMS upgrade file or hotfix file from MySonicWall.

ⓘ **NOTE:** The CMS and all its managed SMA appliances use the same upgrade and hotfix file.

To upgrade the CMS and its managed appliances:

1 On the CMS, go to the **Managed Appliances > Maintain** page.

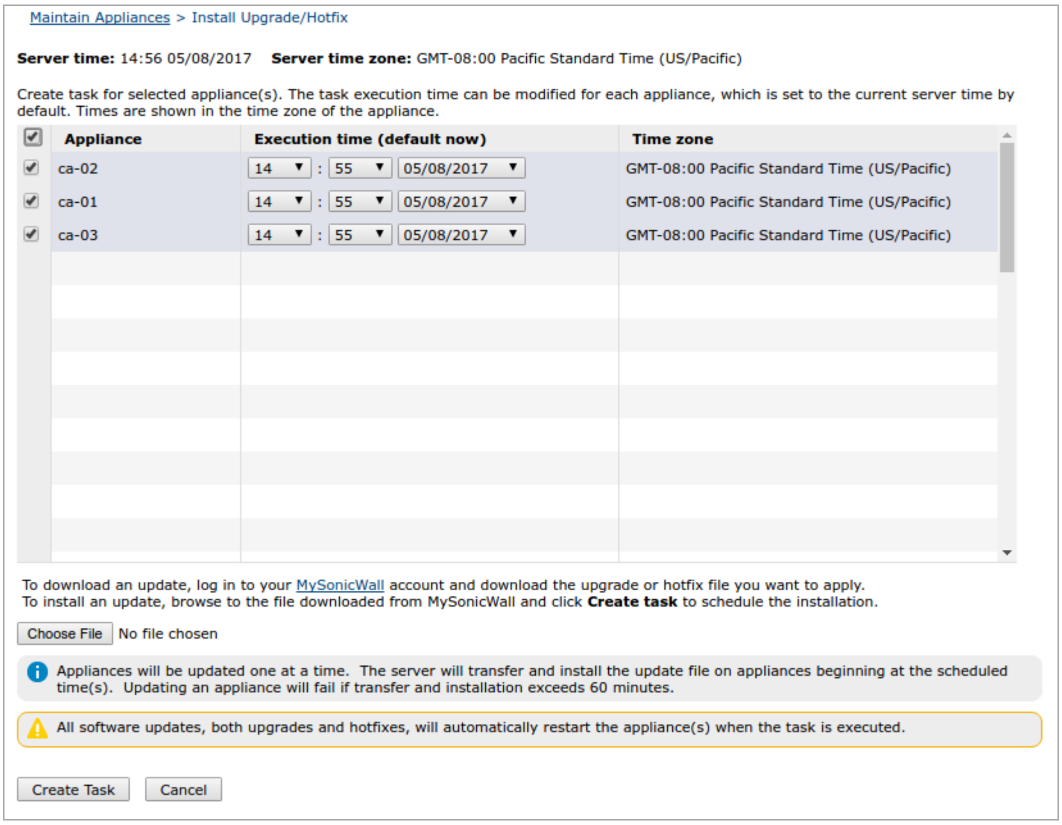


□	Name	Host	Platform	Version	Hotfixes	EPC version	Pending Changes
□	app207	172.24.25.207	SonicWall Secure Mobile Access 8200v	12.1.0-03960	None	17.08.17.12	No
□	app8	172.24.27.8	SonicWall Secure Mobile Access 8200v	12.1.0-03960	None	17.08.17.12	No
□	app9	172.24.27.9	SonicWall Secure Mobile Access 8200v	12.1.0-03960	None	17.08.17.12	No

2 Select the SMA appliance you want to upgrade.

> **NOTE:** You can select multiple appliances to update at the same time.

3 Click **Upgrade/Hotfix**.



Server time: 14:56 05/08/2017 **Server time zone:** GMT-08:00 Pacific Standard Time (US/Pacific)

Create task for selected appliance(s). The task execution time can be modified for each appliance, which is set to the current server time by default. Times are shown in the time zone of the appliance.

☑	Appliance	Execution time (default now)	Time zone
☑	ca-02	14 ▼ : 55 ▼ 05/08/2017 ▼	GMT-08:00 Pacific Standard Time (US/Pacific)
☑	ca-01	14 ▼ : 55 ▼ 05/08/2017 ▼	GMT-08:00 Pacific Standard Time (US/Pacific)
☑	ca-03	14 ▼ : 55 ▼ 05/08/2017 ▼	GMT-08:00 Pacific Standard Time (US/Pacific)

To download an update, log in to your MySonicWall account and download the upgrade or hotfix file you want to apply.
To install an update, browse to the file downloaded from MySonicWall and click **Create task** to schedule the installation.

Choose File No file chosen

Appliances will be updated one at a time. The server will transfer and install the update file on appliances beginning at the scheduled time(s). Updating an appliance will fail if transfer and installation exceeds 60 minutes.

All software updates, both upgrades and hotfixes, will automatically restart the appliance(s) when the task is executed.

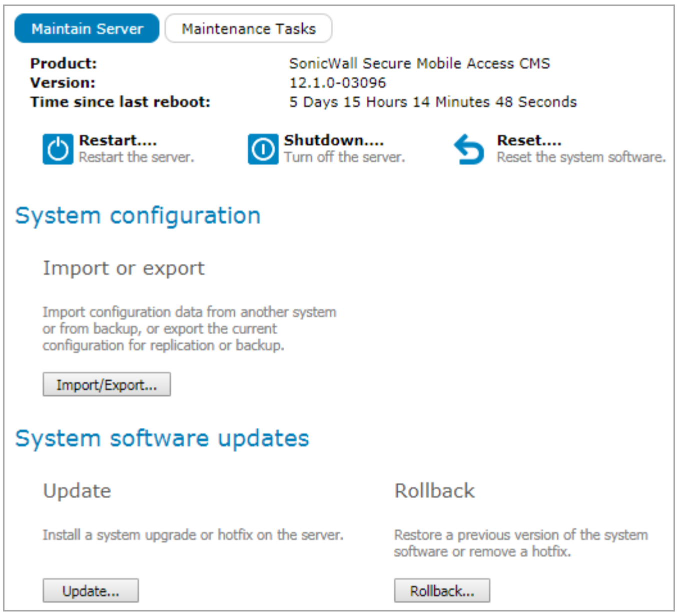
4 Choose a time to upgrade each appliance.

5 Click **Choose File** to select the downloaded upgrade file.

6 Select **Create Task**.

7 Repeat Step 2 through Step 6 for each managed SMA appliance.

8 Once all the managed appliances have been upgraded, go to the **Management Server > Maintain** page.


Maintain Server
Maintenance Tasks

Product: SonicWall Secure Mobile Access CMS
Version: 12.1.0-03096
Time since last reboot: 5 Days 15 Hours 14 Minutes 48 Seconds

Restart.... Restart the server.
Shutdown.... Turn off the server.
Reset.... Reset the system software.

System configuration

Import or export

Import configuration data from another system or from backup, or export the current configuration for replication or backup.

System software updates

Update

Install a system upgrade or hotfix on the server.

Rollback

Restore a previous version of the system software or remove a hotfix.

ⓘ **NOTE:** All managed appliances must be upgraded before CMS can be upgraded.

9 Under **System software updates**, click **Update**.

Verifying the Update

To verify the update:

1 Log in to AMC.

2 From the main navigation menu, navigate to the **System Status**.

3 Verify that the update succeeded by verifying the **Version** number:

12.1-<three-digit build number>

Post-Upgrade Tasks

The following sections review tasks you may need to perform if the upgrade doesn’t complete successfully.

Topics:

- Restoring a Configuration
- Rolling Back to a Previous Version
- Creating/Importing a New Certificate

Restoring a Configuration

If the installation of the update or hotfix file is interrupted or fails, you can restore the configuration you saved earlier in the process.

To restore a configuration:

1. From the main navigation menu in AMC, click **Maintenance**.
2. In the **System configuration** area, click **Import/Export**.
3. In the **File name** field, type the path of the appropriate file, or click **Browse** to locate it.

   ⓘ **NOTE:** The filename format is: *<appliance_name>-<date>-<nnn>.aea*).

4. Click **Import**.
5. To activate the imported configuration, select **Apply Changes**.

Rolling Back to a Previous Version

From AMC, you can undo the most recent update installed on the system. If you experience problems after completing an update, you may want to use this feature to roll back to a known state. Each time you roll back the software image, it removes the most recent system update and restores the version that existed just prior to the update.

△ **CAUTION: If you have made any configuration changes since updating the system, rolling back the software image erases these changes.**

To roll back to a previous version:

1. From the main navigation menu in AMC, click **Maintenance**.
2. In the **System configuration** area, select **Rollback**.
3. To roll back to the version displayed on the Rollback page, click **OK**. After the rollback process is complete, the appliance automatically restarts and applies the changes.
4. After the appliance restarts, verify the new version number in the bottom-left corner of the AMC home page.

Creating/Importing a New Certificate

Users may not be able to connect to the appliance after upgrading to 12.1 because the upgraded appliance has a self-signed/CA-issued certificate with an SHA-512 hash. To resolve this issue, create or import a new certificate with an SHA-256, or SHA-384 hash after upgrading to 12.1.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/contact-support.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. 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/.

Legend

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

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

ⓘ **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 2/14/18

232-002580-00 Rev B