

# SonicWall® Secure Mobile Access 12.4

Upgrade Guide



# Contents

<b>Introduction</b>	<b>3</b>
<b>Upgrade Description</b>	<b>4</b>
Upgrade Summary	4
Platform Compatibility	5
Deprecated Features	5
Unsupported Features	6
<b>Special Considerations</b>	<b>7</b>
Connect Tunnel Upgrade Requirements	7
Upgrading OSPWAT OESIS libraries from V3 to V4	7
<b>Preparation</b>	<b>8</b>
Finding the Authentication Code	8
Registering your SMA Appliance	8
Obtaining the Upgrade File or Hotfix	9
Verifying the Downloaded Upgrade File	9
Backing up your Current Configuration	9
<b>SMA Infrastructure Upgrade</b>	<b>11</b>
Installing an Update or Hotfix Using the Appliance Management Console	11
Upgrading CMS and Managed Appliances	12
Verifying the SMA Update	13
Verifying the CMS Update	14
Verifying the Managed Appliances Update	14
<b>Post-Upgrade Tasks</b>	<b>15</b>
Importing a Configuration	15
Rolling Back SMA to a Previous Version	15
Rolling Back CMS to a Previous Version	16
Creating/Importing a New Certificate	18
<b>SonicWall Support</b>	<b>19</b>
About This Document	20

# Introduction

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](#)
- [Unsupported Features](#)

## Upgrade Summary

To upgrade process for SMA includes, updating both the SMA appliances and the client end points such as SMA clients. 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.  
**i** | **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 upgrade file for your SMA appliance and for the client end points from MySonicWall.
- 4 Upload and install the upgrade file:
  - For standalone appliances: upload and install the upgrade file using the Appliance Management Console (AMC).
  - i** | **NOTE:** The appliance is rebooted as a part of the upgrade process.
  - For CMS managed appliances: upload and install the upgrade file using the Central Management Console (CMC).
  - i** | **NOTE:** All managed appliances must be upgraded before you upgrade the CMS. Upgrading the CMS to 12.4 is allowed only when all of its managed appliances have been upgraded to 12.4.
- 5 Hotfixes are released to patch bugs. There are platform and client hotfixes. They should be applied to the platform first and then the client. Both hotfixes, and also related client upgrades, are necessary to resolve all known issues fixed by that hotfix set.
- 6 Install the client upgrade on all the client endpoints and verify them.

# Platform Compatibility

The SMA supports the following SMA 1000 series appliances running SMA 12.4 firmware:

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

**NOTE:** EX6000, EX7000, and EX9000 appliances cannot be upgraded to SMA 12.4.

You can upgrade a supported SMA appliance directly to version 12.4 from these versions:

- 12.3 + latest hotfixes
- 12.1 + latest hotfixes

**IMPORTANT:**

- To upgrade from SMA 11.4, you must upgrade to version 12.1 first, then upgrade to 12.4.
- To upgrade from SMA 12.2, you must upgrade to version 12.3 first, then upgrade to 12.4.

**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 12.4:

- Support for RSA ClearTrust authentication servers is hidden by default in SMA 12.4. It can, if necessary, be enabled by setting `CEM MGMT_ALLOW_CLEARTRUST=true`.
- Support for Fallback Servers for Network Tunnel clients is hidden by default in SMA 12.4. It can, if necessary, be enabled by setting `CEM MGMT_FALLBACK_SERVERS=true`.
- OPSWAT V3 attributes are no longer supported as V3 libraries are not compatible with the latest antivirus applications and firewalls.
  - If you have OPSWAT V3 attributes configured, upgrading to SMA 12.4 is prevented. To upgrade to SMA 12.4, remove the OPSWAT V3 attributes and proceed with the upgrade process.
  - Importing old configuration with OPSWAT V3 attributes/profiles will block applying “Pending Changes” until those are deleted.
- TLS 1.0 and TLS 1.1 are no longer supported for user sessions.
  - If you have configured TLS transport protocol as “Any TLS version” in prior version of SMA, upgrading to SMA 12.4 is prevented. In order to upgrade to SMA 12.4, select “TLS version 1.2 only” or “TLS version 1.2 or 1.1” in AMC and proceed with the upgrade process.
- Legacy SSO is deprecated and enhanced with Dynamic Single Sign On feature.
  - If you wish to use the Legacy SSO, you can still use by enabling the CEM setting to `AMC_SHOW_LEGACY_SSO_PROFILES=true`

- Connect Tunnel Legacy for Windows 10 is deprecated.

**NOTE:**

For more information on how to use the Legacy client on Windows 10, refer to the *Connect Tunnel User Guide*.

- Windows 7 support is limited as Microsoft has ended their support.

## Unsupported Features

The following features are no longer supported on all SMA 1000 series appliances in SMA 12.4:

- **Virtual Assist**

When you attempt to upgrade to SMA 12.4 from an earlier release or import an older configuration into SMA 12.4 configuration, the system prevents the upgrade or import and notifies you with the following message:

```
Virtual Assist is not available in SMA 12.4. You must disable
Virtual Assist before you can upgrade to SMA 12.4.
```

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 central policy management through the Policy Synchronization feature. 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 12.4, 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 12.4. Attempting to upgrade a node in an HA Pair to SMA 12.4 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 12.4 may not succeed if any virtual hosts with IP addresses are defined in the current configuration. Performing a full import of an older configuration into SMA 12.4 configuration does not succeed, but importing a partial configuration into SMA 12.4 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. Solutions with Connect Tunnel implemented also has special considerations for updating endpoints.

### Topics:

- [Connect Tunnel Upgrade Requirements](#)
- [Upgrading OSPWAT OESIS libraries from V3 to V4](#)

## Connect Tunnel Upgrade Requirements

Client component upgrades follow the same requirements as appliance upgrades. The latest hotfixes for the client components should be applied before the performing the upgrade.

You can upgrade appliance and client components to 12.4 as shown below:

- 12.3 + latest hotfixes -> 12.4
- 12.1 + latest hotfixes -> 12.4



### IMPORTANT:

- To upgrade from Connect Tunnel 11.4, you must upgrade to version 12.1 first, then upgrade to 12.4.
- To upgrade from Connect Tunnel 12.2, you must upgrade to version 12.3 first, then upgrade to 12.4.

After you upload 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 12.1 or higher.

## Upgrading OSPWAT OESIS libraries from V3 to V4

The OESIS V3 libraries have been declared out of support by OPSWAT. 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
- Registering your SMA Appliance
- Obtaining the Upgrade File or Hotfix
- Verifying the Downloaded Upgrade 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 **System Configuration > General Settings** page in the Appliance Management Console (AMC)

## Registering your SMA Appliance

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

**NOTE:** You must have a MySonicWall account in order to register the appliance. If you do not already have a MySonicWall account, navigate to <https://mysonicwall.com> and follow the prompts to create one.

**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 Click on the **Add Product** icon on the far right of your MySonicWall **Dashboard**. The **Quick Register** dialog box displays.
- 4 Enter your serial number, and then click **Confirm**.
- 5 Confirm your serial number.
- 6 Enter a name for this appliance.
- 7 Enter the authentication code.
- 8 Select the Product group to which you want to assign the appliance.
- 9 Click **Register**.
- 10 Follow the online prompts to complete the registration process.



# Obtaining the Upgrade File or Hotfix

*To obtain the upgrade file:*

- 1 Navigate to <https://www.mysonicwall.com>.
- 2 Log in with your MySonicWall username and password.
- 3 On the **Resources & Support > My Downloads** page, select your appliance model from the **My Downloads** list.
- 4 Click the Download icon for the upgrade file or hotfix that you want to download for your appliance.

 **NOTE:** Click the down arrow to view the size of the file.

For a new firmware version, you will be prompted to download a file named *upgrade-<n>\_<n>\_<n>\_<five digit build number>.bin* file to your local computer. Hotfix filenames use the following naming convention: *<component>-hotfix-<version>-<hotfix number>.bin*.

## Verifying the Downloaded Upgrade 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)*.


*To compare checksums using the File Checksum Integrity Verifier:*

- 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 to 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, copy the upgrade file to the appliance and 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, navigate to **System Configuration > Maintenance**.
- 2 In the **System Configuration** section, in the **Import or export** area, click **Import/Export...**
- 3 In the **Export Configuration** section, click the **Export...** button.

 **NOTE:** If you have configured any third party agents, select the **Include third party agents** checkbox and click the **Export** button to back up your third party configurations.

- 4 Click **OK**.
  - 5 If 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 that your appliances are running the latest hotfix. 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 Release Notes to see the most up-to-date hotfix recommendations. To access the Release Notes, log in to **MySonicWall account > Resources & Support > Download Center** and select the corresponding Release Notes.

## Current Hotfixes (as of Publication Date)

Firmware Version	Latest Platform (Appliance) Hotfix	Latest Client Hotfix
12.1	pform-hotfix-latest	clt-hotfix-12.1.0-latest
12.3	pform-hotfix-latest	clt-hotfix-12.1.0-latest

**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 Using the Appliance Management Console](#)
- [Upgrading CMS and Managed Appliances](#)
- [Verifying the SMA Update](#)
- [Verifying the CMS Update](#)
- [Verifying the Managed Appliances Update](#)

## Installing an Update or Hotfix Using the Appliance Management Console

If you have not already downloaded the update or hotfix file, see [Obtaining the Upgrade File or Hotfix](#) for instructions. Save the file to your local system.

- NOTE:**
- If you have OPSWAT V3 attributes configured, upgrading to SMA 12.4 is prevented. To upgrade to SMA 12.4, remove the OPSWAT V3 attributes and proceed with the upgrade process.
  - If you have TLS version 1.0 and 1.1 configured, upgrading to SMA 12.4 is prevented. To upgrade to SMA 12.4, change the TLS version to 1.2 or 1.3 in AMC and proceed with the upgrade process.
  - The upgrade is prevented if Virtual Assist/Replication/GMS is enabled.

### To install the update or hotfix:

- 1 From the main navigation menu in AMC, navigate to the **System Configuration > Maintenance**.
- 2 In the **System Software Updates** section, in the **Update** area, click **Update...**
- 3 Click **Choose File** to locate the update or hotfix file, or type the file path.
- 4 Expand the **Advanced** section if you want to schedule installation of the update or hotfix for a later time.
- 5 Click **Install update**. This step may take several minutes, depending on the network connection speed.

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

If you have any issues after the upgrade, you can roll back the SMA version to the prior version. For more information, see [Rolling Back SMA to a Previous Version](#)

## Upgrading CMS and Managed Appliances

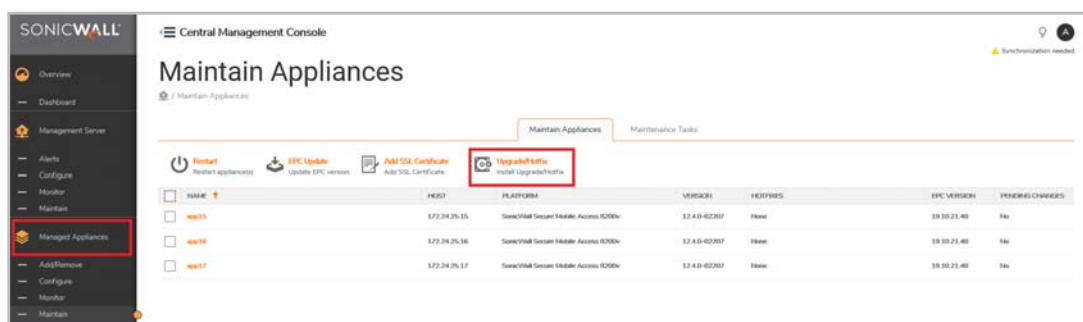
You can use the Central Management Console (CMC) to upgrade and apply hotfixes to your entire VPN infrastructure, including the CMS and all its managed appliances. You can download the CMS upgrade file or hotfix file from MySonicWall.

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

### To upgrade the CMS and its managed appliances:

**NOTE:** All managed appliances must be upgraded before you upgrade the CMS. Upgrading the CMS to 12.4 is allowed only when all of its managed appliances have been upgraded to 12.4.

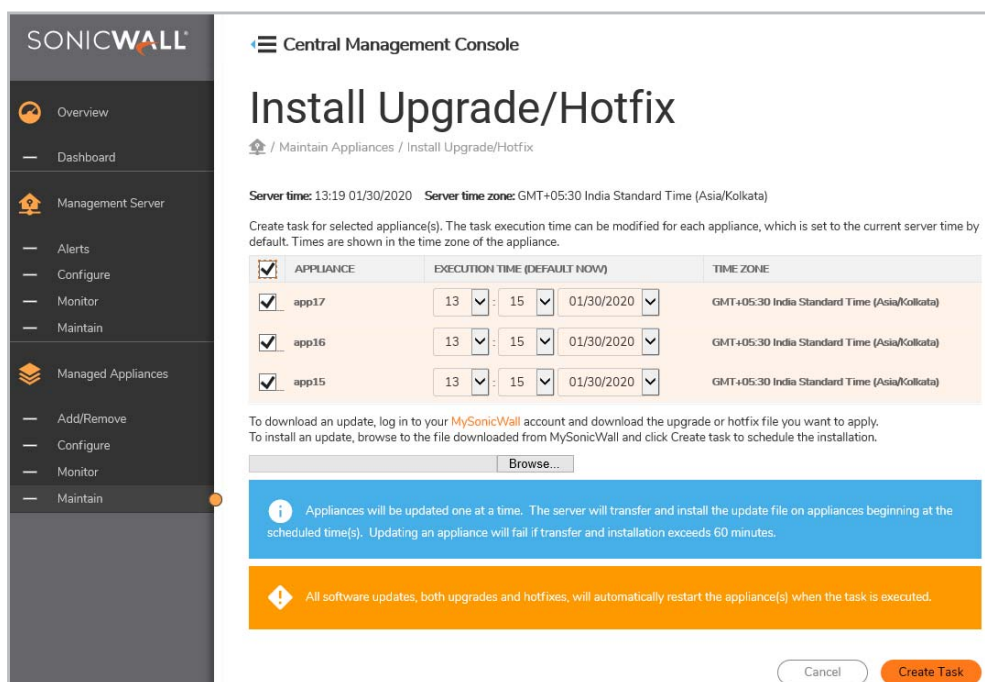
- 1 On the Central Management Console, navigate to **Managed Appliances > Maintain**.



- 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**.
- 4 Choose a time to upgrade each appliance.
- 5 Click **Browse** to select the downloaded upgrade file.
- 6 Select **Create Task**. This will upgrade all the selected managed appliances.



- 7 Once all the managed appliances have been upgraded, navigate to the **Management Server > Maintain** page.
- 8 Under **System Software Updates**, click **Update...**
- 9 Click **Choose File** to select the downloaded upgrade file.
- 10 Expand the **Advanced** section if you want to schedule installation of the update or hotfix for a later time.
- 11 Click **Install update**. This step may take several minutes, depending on the network connection speed.

After the file upload process is completed, the update or hotfix is automatically installed on the CMS. You cannot cancel this part of the installation process. The CMS will automatically restart when the installation of the update or hotfix is completed.

## Verifying the SMA Update

### To verify the SMA update:

- 1 Log in to AMC.
- 2 From the main navigation menu, navigate to **Monitoring > System Status**.
- 3 Verify that the update succeeded by verifying the **Version** number in the **System information** section:  
*12.4.0-<multi-digit build number>*

# Verifying the CMS Update

*To verify the CMS update:*

- 1 Log in to Central Management Console (CMC).
- 2 From the main navigation menu, under **Management Server**, navigate to **Monitor > System Status**.
- 3 Verify that the update succeeded by verifying the **Version** number in the **System information** section  
*12.4.0-<multi-digit build number>*

# Verifying the Managed Appliances Update

*To verify the Managed Appliance update:*

- 1 Log in to Central Management Console (CMC).
- 2 From the main navigation menu, under **Managed Appliances > Maintain**.
- 3 Verify that the update succeeded by verifying the **Version** number in the **Maintain Appliances** tab  
*12.4.0-<multi-digit build number>*

# Post-Upgrade Tasks

These sections describe tasks you may need to perform if the upgrade does not complete successfully.


## Topics:

- [Importing a Configuration](#)
- [Rolling Back SMA to a Previous Version](#)
- [Rolling Back CMS to a Previous Version](#)
- [Creating/Importing a New Certificate](#)

## Importing a Configuration


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

### *To import a configuration:*

- 1 From the main navigation menu in AMC, navigate to **System Configuration > Maintenance**.
- 2 In the **System Configuration** section, in the **Import or Export** area, click **Import/Export....**
- 3 In the **File name** field, click **Choose File** to locate the configuration file.  
 | **NOTE:** The filename format is: `<appliance_name>-<date>-<nnn>.aea`.
- 4 Click **Import**.
- 5 Click the **Pending changes** link to import the saved configuration.
- 6 In the **Apply Pending Changes** prompt, expand the **Advanced** section if you want to schedule the apply changes for a later time.  
OR  
Select **Apply Changes** to activate the imported configuration immediately.

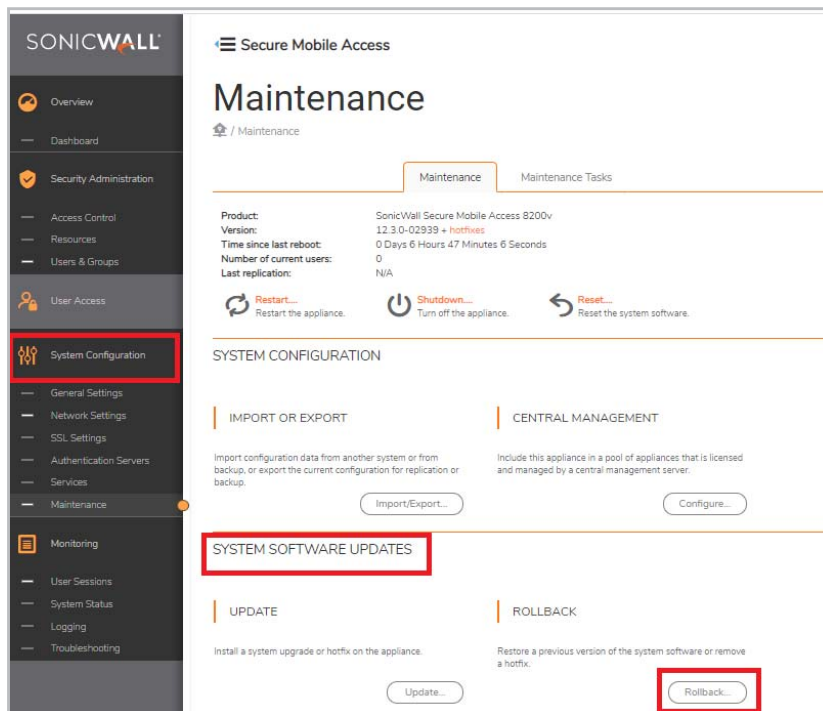
## Rolling Back SMA to a Previous Version

From AMC, you can undo the most recent update installed on the system. If you experience problems after completing an update, you can roll back to the previous version. 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 SMA to a previous version:**

- 1 From the main navigation menu in AMC, navigate to **System Configuration > Maintenance**.
- 2 In the **System Software Updates** section, in the **Rollback** area, select **Rollback....**



- 3 To roll back to the version displayed on the Rollback page, click **Rollback** and then **Yes** to confirm the Rollback.
- After the rollback process completes, the appliance will automatically restart and apply the changes.
- 4 After the appliance restarts, verify the version number in the bottom-left corner of the AMC home page.

## Rolling Back CMS to a Previous Version

From Central Management console, you can undo the most recent update installed on the system. If you experience problems after completing an update, you can roll back to the previous version. 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.

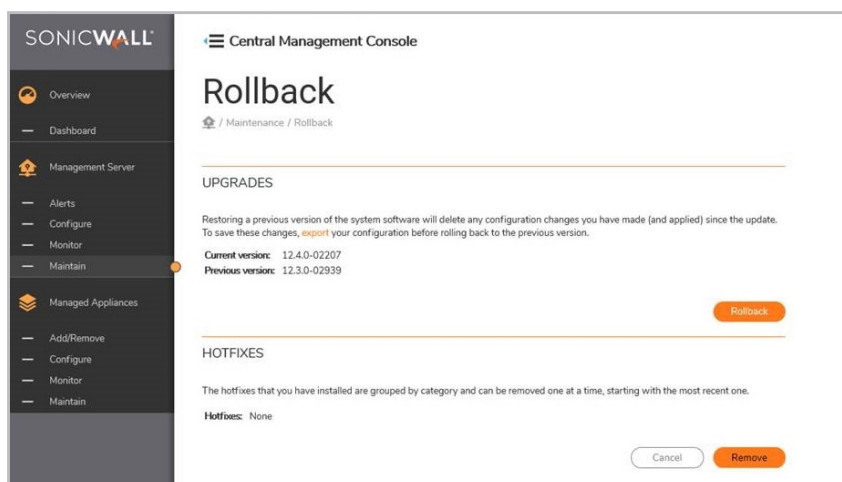
**CAUTION:** If you have made any configuration changes since updating the system, rolling back the software image erases these changes.

To rollback the CMS to a previous version, you should rollback CMS first and then you should roll back all the managed appliances.

**To roll back the CMS to a previous version:**

- 1 On the Central Management Console, navigate to **Management Server > Maintain**.

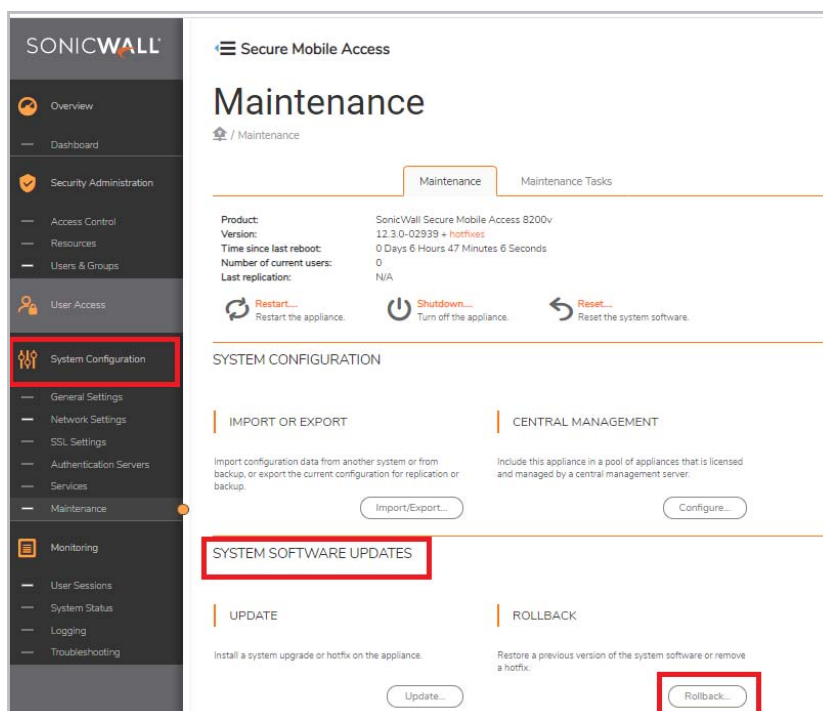




- 2 Under the Upgrades section, click **Rollback**. A pop up window appears you to confirm the rollback.
- 3 In the **Confirm Rollback** pop up window, click **Yes** to confirm the Rollback.  
After the rollback process completes, the CMS will automatically restart and apply the changes.
- 4 After the CMS restarts, verify the version number in the bottom-left corner of the Central Management Console home page.

**To roll back the managed appliance to a previous version:**

- 1 From the main navigation menu in AMC, navigate to **System Configuration > Maintenance**.
- 2 In the **System Software Updates** section, in the **Rollback** area, select **Rollback....**



- 3 To roll back to the version displayed on the Rollback page, click **Rollback** and then **Yes** to confirm the Rollback.  
After the rollback process completes, the appliance will automatically restart and apply the changes.
- 4 After the appliance restarts, verify the 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 SMA12.4 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 either an SHA-256 or SHA-384 hash after upgrading to SMA 12.4.

**NOTE:** For more information on how to create or to import a new certificate, refer to the *SMA Administration Guide*.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid 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://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

# About This Document

## 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, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SMA Upgrade Guide  
Updated - February 2020  
Software Version - 12.4  
232-005236-00 Rev A

## Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

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 reserves 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>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

## Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
SonicWall Inc. Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035