Secure Mobile Access 10.2

Upgrade Guide

for SMA 100

SONICWALL®

Contents

1

Introduction

This Upgrade Guide provides instructions for upgrading your SonicWall® Secure Mobile Access (SMA) 100 Series system from previous versions of Secure Mobile Access firmware to the latest version of SMA 10.2.1. This guide also provides information about importing the configuration settings from an appliance running versions of SMA 9.0.0.10-28v, or 10.2.x to an appliance running SMA 10.2.x. See *Upgrading the Appliance with New Firmware* and *Importing Configuration Settings* for details about the models and firmware versions supported.

Topics:

Knowledge Base Articles for Upgrading

IMPORTANT: Be sure to review the following Knowledge Base articles before upgrading your SMA appliance.

- SMA 100 Series Support Matrix
- How To Upgrade Firmware On SMA 100 Series Appliances
- SMA100: Configuration Migration Tool
- Additional SMA 100 Series 10.X And 9.X Firmware Updates Required
- SMB SSL-VPN: Upgrading Firmware On SMA 500v Virtual Appliance

Obtaining The Latest Secure Mobile Access Firmware

NOTE: Secure Mobile Access 10.2 firmware is only supported on SMA 200, 210, 400, and 410 appliances, and on SMA 500v virtual appliances. Version 10.2 is not available for SRA 1200/1600/4200/4600 or older platforms.

NOTE: If you have already registered your SonicWall SMA appliance, and selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.

To obtain a new Secure Mobile Access firmware image file for your SonicWall appliance:

1. In a browser on your management computer, log into your MySonicWall account at https://www.mysonicwall.com/.
2. In MySonicWall, navigate to **Product Management > My Products** in the left navigation pane to display the list of your registered appliances.
3. Mouse over the row that displays your appliance model. Options appear at the right side of the row.
4. Click the **Firmware** icon.

5. Click **Browse All Firmware** to display all available firmware versions.
    a. Mouse over the row for the firmware you want. Options appear at the right.
    For example:
        - For the SonicWall SMA 410 appliance, this is a file such as:
        `sw_sma410__EN_10.2.1.0-17sv.sig`
        - For the SonicWall SMA 500v for ESXi, this is a file such as:
            - To upgrade an existing SMA 500v for ESXi:
            `sw_smavm__EN_10.2.1.0-17sv.sig`
            - For fresh installation of SMA 500v for ESXi:
            `sw_smavm_eng_10.2.1.0_10.2.1_p_17sv_1268045.ova`

- For the SonicWall SMA 500v for Hyper-V, this is a file such as:
  - To upgrade an existing SMA 500v for Hyper-V:
    `sw_smahyperv__EN_10.2.1.0-17sv.sig`
  - For fresh installation of SMA 500v for Hyper-V:
    `sw_sma_hyperv_eng_10.2.1.0_10.2.1_p_17sv_1268045.vhdx.zip`
    ⓘ | **TIP:** Extract the downloaded zip file to get the `.vhdx` file.
- For the SonicWall SMA 500v for Azure, this is a file such as:
  - To upgrade an existing SMA 500v for Azure:
    `sw_500vazure__EN_10.2.1.0-17sv.sig`
  - For fresh deployment of SMA 500v for Azure, go to the Microsoft Azure Marketplace at https://azuremarketplace.microsoft.com/en-us/marketplace/ and then search for **SonicWall SMA 100**.
- For the SonicWall SMA 500v for AWS, this is a file such as:
  - To upgrade an existing SMA 500v for AWS:
    `sw_500vaws__EN_10.2.1.0-17sv.sig`
  - For fresh installation of SMA 500v for AWS, contact SonicWall Sales at https://www.sonicwall.com/customers/contact-sales or SonicWall Support at https://www.sonicwall.com/support/contact-support. SonicWall provides the **ami** file for the installation.
- For the SonicWallSMA 500v for KVM, this is a file such as:
  - To upgrade an existing SMA 500v for KVM
    `sw_500vkvm__EN_10.2.1.0-17sv.sig`
  - For fresh installation of SMA 500v for KVM:
    `sw_sma_kvm_eng_10.2.1.0_10.2.1_p_17sv_1268045.qcow2`
    ⓘ | **TIP:** Extract the downloaded zip file to get the `.qcow2` file.

ⓘ | **NOTE:** The mentioned firmware file names are for illustrative purpose only. It is advised to upgrade or install to the latest release as the latest firmware has all the latest bug fixes and new features.

6. On MySonicWall, click the **Download** icon to download the firmware to your computer, and click the PDF icon to display the *Release Notes*.

7. For a SMA 500v for Hyper-V fresh installation, extract the VHD file from the downloaded zip file.

Exporting a Copy of your Configuration Settings

Before beginning the update process, export a copy of your SonicWall SMAappliance configuration settings to your local machine. The **EXPORT** option saves a copy of the current configuration settings, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

To save a copy of your configuration settings in SMA 10.2 and export them to a file on your local management station, click **EXPORT** on the **System > Settings** page and save the settings file to your local computer. The default settings file is named **sslvpnsettings-xxxxxxxx.zip** (where xxxxxxx is the serial number of the appliance).

To export the configuration settings from an appliance running SMA 9.0 or earlier, navigate to the **System > Settings** page in the SMA appliance and click **Export Settings**.

TIP: To more easily restore settings in the future, rename the .zip file to include the version of the SonicWall SMA firmware from which you are exporting the settings.

Upgrading the Appliance with New Firmware

This section describes how to upload a new firmware image to the SonicWall SMA appliance and then reboot the appliance with the new firmware.

Firmware upgrade to SMA 10.2.1 is supported from the following previous versions:

- SMA 9.0.0.10-28sv
- SMA 10.2.x

See https://www.sonicwall.com/support/knowledge-base/upgrade-path-for-sma100-series/190314100423452/ for additional information.

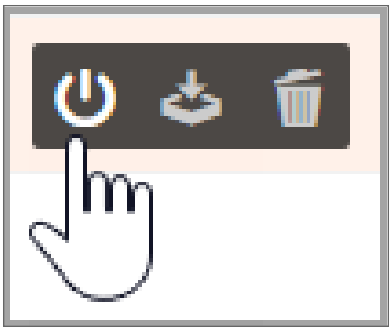
NOTE: SonicWall SMA appliances do not support downgrading to an earlier firmware version and directly rebooting the appliance with the configuration settings from a higher version. If you are downgrading to a previous version of the Secure Mobile Access firmware, you must select **Boot with factory default settings**. You can then import a settings file saved from the previous version or reconfigure manually.

NOTE: SonicWall appliances upgrade to 10.2.X is supported from the SonicWall SMA appliances running 9.0 or 10.2.

To upload a new firmware image and restart the appliance:

1. Download the Secure Mobile Access image file and save it to a location on your local computer.
2. Select **UPLOAD NEW FIRMWARE** from the **System > Settings** page. Browse to the location where you saved the Secure Mobile Access image file, select the file, and click **ACCEPT**. The upload process can take up to one minute.

3. When the upload is complete, you are ready to reboot your SonicWall SMA appliance with the new Secure Mobile Access image. Do one of the following:
    - To reboot the image with current preferences, mouse over the **New Firmware** row and click the boot icon at the right, then click **BOOT** in the **BOOT FIRMWARE** dialog.



    - To reboot the image with factory default settings, mouse over the New Firmware row and click the boot icon at the right, select the Boot with factory default settings option, and then click **BOOT** in the **BOOT FIRMWARE** dialog.

    NOTE: Be sure to save a backup of your current configuration settings to your local computer before rebooting the SonicWall SMA appliance with factory default settings, as described in the *Exporting a Copy of your Configuration Settings* section.

4. After clicking **BOOT**, do not power off the device while the image is being uploaded to the flash memory.
5. After your SMA appliance successfully restarts with the new firmware, the login screen is displayed. The updated firmware information is displayed on the **System > Status** page and in the **Current Firmware** row on the **System > Settings** page.

Resetting the SMA Physical Appliance using SafeMode

If you are unable to connect to the SonicWall SMA physical appliance web management interface, you can restart the appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

The SafeMode procedure uses a recessed **SafeMode** button in a small pinhole near the power button on the front of the SonicWall appliance.

To reset the SMA appliance in SafeMode

1. Connect your management station to the X0 port on the SonicWall SMA appliance and configure your management station IP address with an address on the `192.168.200.0/24` subnet, such as `192.168.200.20`.

    NOTE: The SonicWall SMA appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.

2. Use a narrow, straight object, like a straightened paper clip or a pen tip, to press and hold the **SafeMode** button on the security appliance for five to ten seconds. The **SafeMode** button is on the front panel in a small hole to the right of the USB connectors.

   TIP: If this procedure does not work while the power is on, turn the unit off and on while holding the **SafeMode** button until the Test light starts blinking.

3. Connect to the SafeMode management interface by pointing the web browser on your management station to http://192.168.200.1. The SafeMode management interface displays.
4. Try rebooting the SonicWall security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.
5. After the SonicWall security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the SafeMode button to restart the appliance in SafeMode again. In SafeMode, restart the Secure Mobile Access image with the factory default settings. Click the boot icon for **Current Firmware** and select the **Boot with factory default settings** option.

Importing Configuration Settings

You can import configuration settings from one appliance to another, which can save a lot of time when replacing an older appliance with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings.

Importing configuration settings, or preferences (“prefs”), to SonicWall appliances running SMA 10.2 is generally supported from the following SonicWall SMA appliances running 9.0 or 10.2:

- SMA 410
- SMA 400
- SMA 210
- SMA 200
- SMA 500v for ESXi
- SMA 500v for Hyper-V
- SMA 500v for Azure
- SMA 500v for AWS
- SMA 500v for KVM

Skipping versions when importing settings is not recommended. See the SMA Configuration Import/Export Support by Firmware Version table for the supported scenarios before importing settings between versions.

For more information about migrating configuration settings or upgrading from older firmware versions to newer ones, refer to this Knowledge Base article:

https://www.sonicwall.com/support/knowledge-base/sma-100-series-support-matrix/170502818222962/

To import configuration settings to an appliance running SMA 10.2, navigate to the **System > Settings** page and click **IMPORT**. Select the settings file to import the saved settings and restart the SMA appliance. You can enable

the **Import the settings partially** option to prevent overwriting some settings on your appliance, including interfaces, routes, DNS, WINS, and licenses.

The tables in the following sections provide details about which firmware versions or which models support importing configuration settings to other Secure Mobile Access 100 Series models and firmware.

- SMA Versions Supporting Configuration Import
- Platform Configuration Import Support Table

NOTE: As the SMA 100 Series and the SMA 1000 Series are different product lines, they do not run the same firmware. At this time, the SMA 100 Series platforms can run SMA 10.2.x. The SMA 1000 Series platforms have different software and they run SMA 12.x.

SMA Versions Supporting Configuration Import

The following table illustrates the supported source and destination versions of SMA when importing configuration settings from one appliance to another.

SMA CONFIGURATION IMPORT/EXPORT SUPPORT BY FIRMWARE VERSION

From	To	
	SMA 9.0	**SMA 10.2**
SMA 9.0	Y	Y
SMA 10.2	N	Y

NOTE: Downgrading versions is not supported.

Platform Configuration Import Support Table

The table in this section shows the SonicWall SMA appliances whose configuration settings can be imported to SonicWall SMA platforms running SMA 10.2.1. The source SMA appliances are in the left column, and the destination SMA appliances are listed across the top.

The legend for this table is:

Y	Supported
N	Unsupported

SMA CONFIGURATION SETTINGS IMPORT SUPPORT BY PLATFORM

		Destination Appliances								
		SMA 200	SMA 210	SMA 400	SMA 410	SMA 500v for ESXi	SMA 500v for Hyper-V	SMA 500v for Azure	SMA 500v for AWS	SMA 500v for KVM
S	SMA 200	Y	Y	N	N	N	N	N	N	N
O	SMA 210	Y	Y	N	N	N	N	N	N	N
U	SMA 400	N	N	Y	Y	N	N	N	N	N
R	SMA 410	N	N	Y	Y	N	N	N	N	N
C	SMA 500v for ESXi	N	N	N	N	Y	Y	N	N	N
E	SMA 500v for Hyper-V	N	N	N	N	Y	Y	N	N	N
	SMA 500v for Azure	N	N	N	N	N	N	Y	Y	Y
	SMA 500v for AWS	N	N	N	N	N	N	Y	Y	Y
	SMA 500v for KVM	N	N	N	N	N	N	Y	Y	Y

NOTE: Underlying hypervisor capabilities such as clustering, import/export, Live Migration (Hyper-V), or vMotion (ESXi), and so on are supported on the SMA500v.

NOTE: High Availability does not function correctly on an SMA 500v after importing HA configuration settings from an SMA 400. You must configure HA directly on the SMA 500v HA pair.

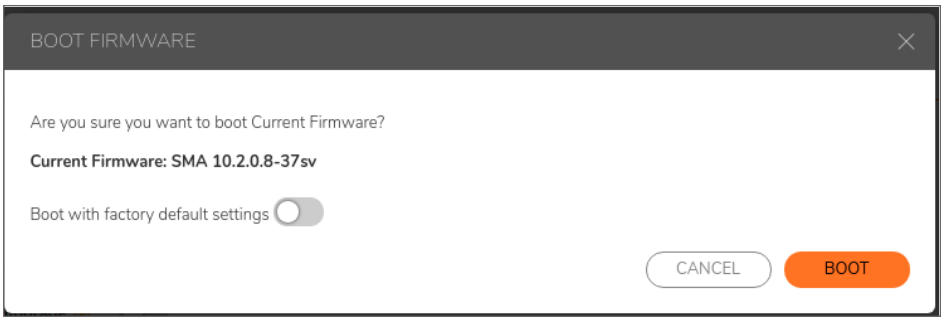
SMA CONFIGURATION IMPORT/EXPORT SUPPORT BY APPLIANCE VERSION

SMA 100 Series Appliance	9.x	10.x	10.2.0	10.2.1
SMA 200	Y	Y	Y	Y
SMA 210	Y	Y	Y	Y
SMA 400	Y	Y	Y	Y
SMA 410	Y	Y	Y	Y
SMA 500v (ESXi)	Y	Y	Y	Y
SMA 500v (Hyper-V)	N	Y	Y	Y
SMA 500v (AWS)	N	N	Y	Y
SMA 500v (Azure)	N	N	Y	Y
SMA 500v (KVM)	N	N	N	Y

Resetting SMA to Factory Default Settings

To reset your SMA to its factory default settings:

1. Navigate to **System > Settings**.
2. Under **Settings Management**, click **Export Settings** and file settings file locally.
3. Under the **Firmware Management | Current Firmware** hover over the firmware and click the **I/O** button. The **BOOT FIRMWARE** window appears.
4. On the **BOOT FIRMWARE** window, switch the toggle to enable the **Boot with factory default settings**.



5. Click **Boot**.

2

SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- 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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

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

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

Secure Mobile Access Upgrade Guide for the SMA 100 Series
Updated - January 2022
Software Version - 10.2
232-005200-00 Rev C

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

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

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