Dell™ Secure Mobile Access 11.3.0 Upgrade Guide

October 2015

This document describes the process of obtaining your Dell™ Secure Mobile Access (SMA) firmware update file, verifying it, and installing it on an existing appliance.

- Upgrading Dell™ Secure Mobile Access Firmware to 11.3.0
- Platform compatibility
- Appliance upgrade requirements
- Client upgrade requirements
- Creating a MySonicWALL account
- Registering your Dell SMA appliance
- Finding the authentication code for your appliance
- Obtaining the update file or hotfix from MySonicWALL
- Installing an update or hotfix using AMC
- Verifying the update
- Updating a clustered pair
- Creating/importing a new certificate
- Accessing Web Proxy Agent
- About Dell

Upgrading Dell Secure Mobile Access Firmware to 11.3

This document describes the process of obtaining your Dell Secure Mobile Access (SMA) firmware update file, verifying it, and installing it on an existing appliance.

Updating a clustered pair of Dell Secure Mobile Access appliances is described at the end of this document. For a complete list of known issues from previous versions that are fixed in this release, see the *Release Notes*.

To update the firmware on your Secure Mobile Access appliance, you will need to perform the following tasks:

- Create a MySonicWALL account, if you don't already have one. You need an account in order to register your Secure Mobile Access appliance. MySonicWALL registration information is not sold or shared with any other company.
- Register your device on MySonicWALL. Registration provides access to essential resources, such as your license file, firmware updates, documentation, and technical support information. When you register, you are prompted to enter an authentication code.
- Use your MySonicWALL account to retrieve the update file for your Secure Mobile Access appliance.
- Upload the update file to your appliance using the Appliance Management Console (AMC) and then click Install Update, which will reboot the appliance.
- Obtain your client component update file, install it to all client endpoints, and verify it.

Platform compatibility

Version 11.3.0 Secure Mobile Access firmware is supported on the following appliances:

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

Appliance upgrade requirements

You can upgrade your Secure Mobile Access appliance directly to version 11.3.0 from the following versions when the most recent Hotfix has been installed:

- When upgrading to 11.3.0 from the same major release version (11.X), we support upgrades from the three previous versions. For example, you can upgrade to 11.3.0 directly from 11.2.0 or 11.1.0.
- When upgrading to 11.3.0 from the previous major release version (10.7.X), you can upgrade to 11.3.0 directly from 10.7.2.

NOTE: Upgrading the Central Management Server (CMS) from 11.2.0 to 11.3.0 is not supported.

It is a best practice that the appliance be running the latest Hotfix version before upgrading from the versions listed above. The most recent Hotfix list for each firmware version as of the date of these Release Notes is shown below. It is possible that additional hotfixes will be released for these versions. In which case, you can access the corresponding Knowledge Base link to see the most up-to-date hotfix recommendations.

Table 1. Latest hotfixes

Firmware Version	Latest Platform (Appliance) Hotfix	Latest Client Hotfix	Knowledge Base Article
11.2.0	Pform-hotfix-11.2.0-269	Clt-hotfix-11.2.0-269	SW13951
11.1.0	Pform-hotfix-11.1.0-227	Clt-hotfix-11.1.0-227	SW12495
10.7.2	Pform-hotfix-10.7.2-392	Clt-hotfix-10.7.2-392	SW13949

To check whether any hotfixes have been applied, click **System Status** or **Maintenance** from the main navigation menu in AMC. If any hotfixes have been incorporated, you'll see a **hotfixes** link next to the version number. Click the link for more information about which ones have been applied.

Client upgrade requirements

Client component upgrades follow the same requirements as appliance upgrades.

If hotfixes are up to date on the client, you can upgrade your client components directly to version 11.3.0 from any of the following versions:

- 11.2.0 + Hotfixes –> 11.3.0
- 11.1.0 + Hotfixes –> 11.3.0
- 10.7.2 + Hotfixes –> 11.3.0

Just as you are advised to install all currently available hotfixes before upgrading the appliance, the associated client-side fixes need to be installed on all client machines prior to starting the client component upgrade to the next release. After you apply the client hotfix to your appliance, the client-side fixes are pushed to each client machine as it connects to the appliance. Depending on your environment, it can take a few days, weeks, or months before all clients have connected to the appliance and received the client-side fixes.

After you upgrade your appliance to 11.3.0, client components are automatically upgraded as client machines connect to the appliance. Any clients that connect who did not receive the client-side fixes might or might not be upgraded without problems.

Backwards compatibility is supported for all 11.3.0 client access agents with the releases eligible for direct upgrade, listed above. For example, if you upgrade your clients and appliance to version 11.3.0, then notice some type of issue that requires you to roll the appliance back to 11.2.0 (with hotfixes), the 11.3.0 client access agents will still activate correctly when the client connects to the 11.2.0 appliance.

Creating a MySonicWALL account

If you do not already have a MySonicWALL account, create one by completing an online registration:

1. In your Web browser, go to https://www.mysonicwall.com.
2. In the User Login section, follow the link for users who are not yet registered.
3. Enter your account information, personal information, and preferences, and then click **Submit**. Be sure to use a valid email address.
4. Follow the prompts to finish creating your account. Dell SonicWALL will send 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 Dell SMA appliance

To register your appliance, perform the following steps:

1. In your Web browser, go to https://www.mysonicwall.com and log in with your username and password.
7. Locate your software serial number, which is printed on the back of your Dell SonicWALL appliance.
8. Enter your serial number, and then click **Next**. Follow the on-screen instructions.
9. Confirm your serial number.
10. Enter a name for this appliance.
11. Click **Register** to continue.
12. Follow the online prompts to fill out the survey and complete the registration process.

Finding the authentication code for your appliance

Your authentication code is the hardware identifier for your appliance, and it is displayed in the following places:

- On the appliance label
- On the **General Settings** page in AMC

Obtaining the update file or hotfix from MySonicWALL

The next step is to obtain the update file and copy it to the file system of your local computer:

1 In your Web browser, go to https://www.mysonicwall.com and log in with your username and password.

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

14 In the **Available Software** list, select the firmware item that corresponds to your appliance. For a new firmware version, you'll be 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*

Verifying the downloaded update file

To make sure 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
```

15 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.

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
```

Installing an update or hotfix using AMC

This section outlines the process of updating your system from AMC with a new firmware version or a hotfix.

- Backing up your current configuration
- Installing the update or hotfix file
- Restoring a configuration
- Rolling back to a previous version

Backing up your current configuration

Before updating, it's a good idea to back up the current configuration data from your appliance using the export feature in AMC. This step is optional, but recommended:

1. From the main AMC navigation menu, click **Maintenance**.
2. In the **System configuration** area, click **Import/Export**.
3. Click the **Export** button. A **File Download** dialog box prompts you to open the *.aea* file or 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**.

4. Click **Save**, browse to the correct directory on your hard drive, and then save the *.aea* file.
5. Click **OK** on the **Export Configuration** page to return to the **Import/Export** page.

Installing the update or hotfix file

Next, install the update or hotfix using AMC:

1. From the main navigation menu in AMC, click **Maintenance**.
2. In the **System software updates** area, click **Update**.
3. If you have not already downloaded the update or hotfix file (as described in the ***Obtaining the Update File or Hotfix from MySonicWALL*** section), click the **mySonicWALL.com** link and log in to download the appropriate update or hotfix file to your local file system.
4. Click **Browse** to locate the update or hotfix file or type the file path.
5. Click **Install Update**. This step may take several minutes, depending on the network connection speed.
6. 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.

Restoring a configuration

If the installation of the update or hotfix file is interrupted or fails, restore a saved configuration (creating a backup, as described in *Backing up your current configuration*, is highly recommended).

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 (*<appliance_name>-<date>-<nnn>.aea*), or click **Browse** to locate it.
4. Click **Import**. To activate the imported configuration, you must 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 will erase 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, click **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.

Verifying the update

After installing the update, verify the current version number in AMC:

1 Log in to AMC.

2 From the main navigation menu, click **System Status** and make sure that the update succeeded by verifying the **Version** number:

11.3.0-<three-digit build number>

Updating a clustered pair

To update the Dell Secure Mobile Access firmware in a cluster environment, you must install the update or hotfix file and import the license file to each node of the cluster. The order in which you update the nodes in the cluster is very important: begin the process with the master node, and then proceed to the slave node. There may be some disruption to service when performing the update, so schedule it using a maintenance window. Be sure to match the serial number and authentication code on MySonicWALL for each appliance; both are displayed on the **Manage Licenses** page in AMC (click **General Settings**, and then click **Edit** in the **Licensing** area).

For more information on managing a cluster, see the *Dell Secure Mobile Access 11.3 Administration Guide*.

To update a cluster:

1. Log in to AMC and verify which node is the Active node (node 1). For more information, see "Monitoring a Cluster" in the *Dell Secure Mobile Access 11.3 Administration Guide*.
2. Log in to AMC on the Active node and then, from the main navigation menu in AMC, click **Maintenance**.
3. In the **System software updates** area, click **Update**.
4. If you have not already downloaded the update file (as described the ***Obtaining the Update File or Hotfix from MySonicWALL*** section), click the **mySonicWALL.com** link, log in, and download the appropriate update or hotfix file to your local file system.
5. Click **Browse** to locate the update or hotfix file or type the file path.
6. Click **Install Update**.

7. While node 1 is updating, the Standby node (node 2) continues servicing requests. When the update to node 1 completes and node 1 comes back online, it notices that the node 2 version differs from its own. It then stops the services on node 2 and services all incoming requests itself.
8. When the update to node 2 completes and node 2 comes back online, it rejoins the cluster and is synchronized with node 1. The cluster is then aware that both nodes are available to service requests.
9. Make sure the update succeeded by verifying in AMC on both nodes that the **Version** number is *11.3.x-<build number>* where *x-<build number>* is the current maintenance release version and three-digit build number. For example, if you update the system with upgrade 11.3.0-258.bin, the version in AMC is reported as 11.3.0-258. Hotfixes do not modify the AMC reported version. For hotfix information, click the **hotfixes** link next to the version number.

Stand-alone system to an HA cluster configuration

You must have two standalone appliances to configure an HA cluster, and the two standalone appliances must be interconnected via the **eth2** interface prior to running the Setup wizard.

When the AMC of the active node comes up, partial import of the stand-alone configuration backup can be done. Once the partial configuration import is successful, the active node synchronizes the configuration with the standby node.

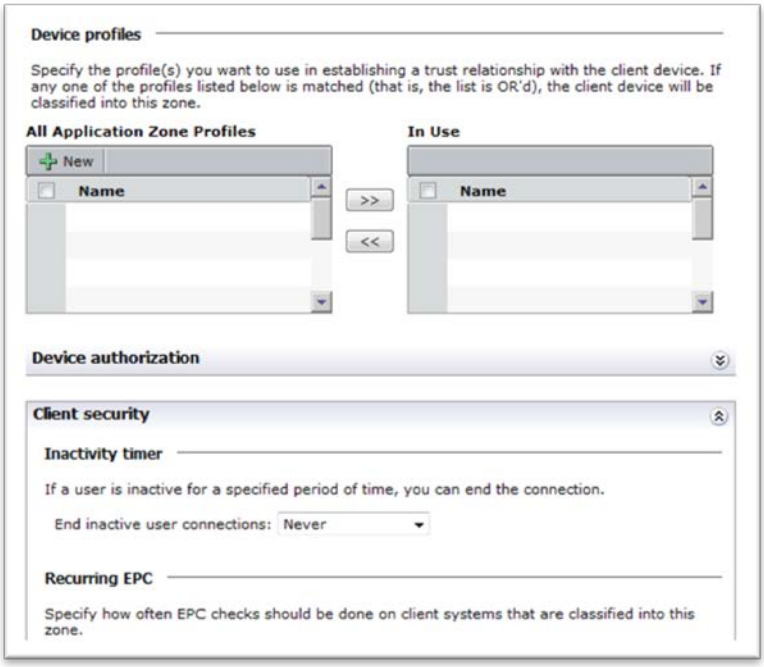
To convert a stand-alone system to an HA cluster configuration:

1. Back up your configuration.
2. In AMC, browse to Maintenance > Reset.
3. Select **Reset the current configuration**, and click **Reset**.
4. Once the system restarts, log in to the Serial Console to run the Setup Wizard again.
5. When prompted if the appliance should be configured as HA, select **Yes**.
6. Once the Setup Wizard is completed on the console, log in to AMC and finish running the Setup Wizard.
7. Once AMC is done with the Setup Wizard and applies changes, log in and import your saved configuration.

NOTE: Be sure to do a Partial Import, as you cannot fully restore a stand-alone configuration backup to an HA-enabled system and vice-versa.

Adjusting the Inactivity Timer

In 11.3.0, the prompt to set the Client Security inactivity timer is on the **Realms > Configure Realm > Configure Community** page to the End Point Control > New Zone Definition page.



Creating/importing a new certificate

Users may not be able to connect to the appliance after upgrading to 11.3.0, 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 a SHA-1, SHA-256, or SHA-384 hash after upgrading to 11.3.0.

Accessing Web Proxy Agent

Web Proxy Agent will no longer be supported after the Secure Mobile Access 11.x series. Therefore, as part of the phase out process, the Web Proxy agent is visible when Secure Mobile Access is upgraded from a previous version where it was enabled. In that case, a warning message appears next to the Access Agents settings, indicating that Web Proxy is entering limited retirement mode, and it is strongly recommended that you remove Web Proxy from the configuration.

For new 11.0.0 and higher installations, Web Proxy is completely hidden. To display the Web Proxy Agent section, specify **?&advanced=1** in the URL.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

For more information about patents, go to http://software.dell.com/legal/patents.aspx.

Trademarks

Dell, the Dell logo, SonicWALL and Aventail are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

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.

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

Last updated: 10/7/2015

232-003008-00 Rev A