



Dell™ SonicWALL™ Secure Mobile Access 8.5.0.4

Release Notes

December 2016

These release notes provide information about the Dell™ SonicWALL™ Secure Mobile Access 8.5.0.4 release.

Topics:

- [About Secure Mobile Access 8.5.0.4](#)
- [Supported platforms](#)
- [Resolved issues](#)
- [Known Issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [About Dell](#)

About Secure Mobile Access 8.5.0.4

Secure Mobile Access (SMA) 8.5.0.4 is a maintenance release that includes several resolved issues for Dell SonicWALL SMA 400, SMA 200, SRA 4600, SRA 1600, and SMA 500v Virtual Appliance (formerly SRA Virtual Appliance).

Supported platforms

The SMA 8.5.0.4 release is supported on the following Dell SonicWALL platforms:

- SMA 400
- SMA 200
- SRA 4600
- SRA 1600
- SMA 500v Virtual Appliance

The SMA 500v Virtual Appliance is supported for deployment on VMware ESXi 5.0 and higher.

NOTE: The SMA 500v Virtual Appliance is not supported on VMware ESX/ESXi 4.0 or 4.1. If you deploy the Virtual Appliance on one of these versions, it should still work, but you might see some warning messages.

Resolved issues

This section contains a list of issues resolved in this release.

Authentication

Resolved issue	Issue ID
Basic authentication is missing from logon requests. Occurs when using application offloading with SRA.	178764
Authentication to RADIUS backup server fails. Occurs when using 2-factor authentication (password + token) with Dell Defender solution.	178697
Authentication with a password containing special characters fails. Occurs when SMTP Authentication is enabled; all characters after the special characters are deleted.	178072
Authentication fails with a Kerberos (authentication) error on the SRA 4600. Occurs when the host list reaches the maximum limit for the list.	170431

Bookmarks

Resolved issue	Issue ID
Cannot upload files if the file path exceeds 130 characters although an error message is not displayed. Occurs when access is through a CIFS bookmark.	180344
A proxy URL breaks native RDP bookmarks. Occurs when an Automatic Proxy Configuration URL is used to set the internet Proxy.	179811
Cannot connect to an RDP native bookmark. Occurs when using MAC OS.	179784

Endpoint Control

Resolved issue	Issue ID
On an SRA 4600, Endpoint Control does not detect the Symantec Endpoint Protection Client and clients are not allowed to connect. Occurs when Symantec Endpoint Protection is installed on a Mac OS X machine.	164999

HTML5

Resolved issue	Issue ID
All files do not download. Occurs when multiple files are downloaded at one time.	179392
Cannot connect while accessing RDP HTML bookmarks. Occurs when trying to access the bookmarks after updating to 8.5 firmware.	179092

Resolved issue	Issue ID
HTML5 bookmarks do not relay diacritic characters (for example, ä ë ï ö ü ÿ) to remote machines. Also, when accessing word processing applications (for example, Word, Notepad, Outlook), the cursor appears as a colon. Occurs when users with US international keyboard layout on the local machine, bookmark, and remote machine connect via an HTML5 bookmark.	174558

NetExtender

Resolved issue	Issue ID
NetExtender does not launch even though SMA Connect Agent connects to the port successfully. Occurs when connecting to a port other than 443 even though the firewall has a NAT rule that translates the other port to 443.	177863

SSL

Resolved issue	Issue ID
Cannot disable TLS 1.0 and TLS 1.1 for generic offloading. Occurs when selecting TLS 1.2 for generic offloading and disabling TLS 1.0/1.1. TLS 1.0 is not disabled and is used instead of TLS1.2 for generic offloading.	177863

Single Sign-on (SSO)

Resolved issue	Issue ID
Single Sign-On does not work with Native Bookmarks. Occurs when using a password with the Swedish characters, ÅÄÖåäö.	179740
Domain information is not included in SSO login information for Citrix bookmarks. Occurs when a Citrix bookmark is created with the SSO option, Use SSL VPN account credentials, enabled and the Citrix StoreFront is configured for access via SRA.	179546
Single Sign-On does not work with application offloading. Occurs when application offloading is configured through the Wizard on an SMA 400.	179069

Upgrade

Resolved issue	Issue ID
Device information is not recorded when you log in after setting up your device management. Occurs when you upgrade from version 8.1.0.3 to 8.5.	178394

Vulnerability

Resolved issue	Issue ID
The Secure Remote Access server is vulnerable to a Remote Command Injection vulnerability in its web administrative interface. Occurs in the component responsible for processing SSL certificate information.	180506
The Secure Remote Access server is vulnerable to a Remote Command Injection vulnerability. Occurs in the component responsible for handling some of the server's internal configurations.	180505
A command injection allows users with access to a web administration console to leverage full control of the machine. Occurs in the component responsible for processing SSL certificate information.	180504

Known Issues

This section contains a list of known issues in this release.

Endpoint Control

Known issue	Issue ID
The EPC check fails with the Mac personal firewall. Occurs when any product is selected.	174192

System compatibility

Topics:

- [Feature support by platform](#)
- [NetExtender client versions](#)
- [Virtual Assist and Virtual Meeting client versions](#)

Feature support by platform

Although all SMA/SRA appliances support major Secure Mobile Access features, not all features are supported on all SMA/SRA appliances.

The Dell SonicWALL SMA/SRA appliances share most major Secure Mobile Access features, including:

- Virtual Office
- NetExtender
- Secure Virtual Assist
- Secure Virtual Access
- Application Offloading
- Web Application Firewall
- Geo-IP
- Botnet
- End Point Control
- Load Balancing



NOTE: HTML5 SSH and Telnet are not supported with Internet Explorer 10 in SMA 8.5.

Features not supported on SMA 200 and SRA 1600

The following features are supported on the SMA 400 and SRA 4600, but not on the SMA 200 or SRA 1600:

- Application Profiling
- High Availability
- Virtual Meeting

NetExtender client versions

The following is a list of NetExtender client versions supported in this release.

Description	Version
NetExtender Linux RPM 32-Bit	8.5.797
NetExtender Linux RPM 64-Bit	8.5.797
NetExtender Linux TGZ 32-Bit	8.5.797
NetExtender Linux TGZ 64-Bit	8.5.797
NetExtender MacOSX	8.5.788
NetExtender Windows	8.5.251

Virtual Assist and Virtual Meeting client versions

The following is a list of Virtual Assist and Virtual Meeting client versions supported in this release.

Description	Version
Virtual Assist Linux RPM	8.5.0.49
Virtual Assist Linux TGZ	8.5.0.49
Virtual Assist MacOSX	8.5.0.2
Virtual Assist Windows	8.5.0.3
Secure Virtual Meeting MacOSX	8.5.0.3
Virtual Meeting Windows	8.5.0.3

Product licensing

The Dell SonicWALL Secure Mobile Access 8.5.0.4 firmware provides user-based licensing on Dell SonicWALL SMA/SRA appliances. Licensing is controlled by the Dell SonicWALL license manager service, and you can add

licenses through their MySonicWALL accounts. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWALL.

License status is displayed in the Secure Mobile Access management interface, on the Licenses & Registration section of the **System > Status** page. The TSR, generated on the **System > Diagnostics** page, displays both the total licenses and active user licenses currently available on the appliance.

If a user attempts to log into the Virtual Office portal and no user licenses are available, the login page displays the error, “No more User Licenses available. Please contact your administrator.” The same error is displayed if a user launches the NetExtender client when all user licenses are in use. These login attempts are logged with a similar message in the log entries, displayed in the **Log > View** page.

To activate licensing for your appliance:

- 1 Log in as admin, and navigate to the **System > Licenses** page.
- 2 Click the **Activate, Upgrade or Renew services** link. The MySonicWALL login page is displayed.
- 3 Type your MySonicWALL account credentials into the fields to log into MySonicWALL. This must be the account to which the appliance is, or will be, registered. If the serial number is already registered through the MySonicWALL web interface, you will still need to log in to update the license information on the appliance itself.

MySonicWALL automatically retrieves the serial number and authentication code.
- 4 Type a descriptive name for the appliance into the **Friendly Name** field, and then click **Submit**.
- 5 Click **Continue** after the registration confirmation is displayed.
- 6 Optionally upgrade or activate licenses for other services.
- 7 After activation, view the **System > Licenses** page on the appliance to see a cached version of the active licenses.

Upgrading information

This section provides information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and resetting your appliance using SafeMode.

Topics:

- [Obtaining the latest Secure Mobile Access firmware](#)
- [Exporting a copy of your configuration settings](#)
- [Upgrading the appliance with new firmware](#)
- [Resetting the SMA/SRA appliance using SafeMode](#)
- [Moving an SMA 500v Virtual Appliance to SMA 8.5.0.4](#)

Obtaining the latest Secure Mobile Access firmware

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

- 1 Log into your MySonicWALL account at <http://www.mysonicwall.com/>.

i **NOTE:** If you have already registered your Dell SonicWALL SMA/SRA 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.

- 2 In MySonicWALL, click **Downloads** in the left navigation pane to display the Download Center screen.
- 3 Select your product in the **Software Type** drop-down list to display available firmware versions.
- 4 To download the firmware to your computer, click the link for the firmware version you want and save it to a location on your management station:
 - For the Dell SonicWALL SMA 400 appliance, this is a file such as:
`sw_sma400_eng_8.5.0.4_8.5.0_p_18sv_946063.sig`
 - For the Dell SonicWALL SMA 200 appliance, this is a file such as:
`sw_sma200_eng_8.5.0.4_8.5.0_p_18sv_946063.sig`
 - For the Dell SonicWALL SRA 4600 appliance, this is a file such as:
`sw_sra4600_eng_8.5.0.4_8.5.0_p_18sv_946063.sig`
 - For the Dell SonicWALL SRA 1600 appliance, this is a file such as:
`sw_sra1600_eng_8.5.0.4_8.5.0_p_18sv_946063.sig`
 - For the Dell SonicWALL SMA 500v Virtual Appliance, this is a file such as:
`sw_smavm_eng_8.5.0.4_8.5.0_p_18sv_946063.sig`

Exporting a copy of your configuration settings

Before beginning the update process, export a copy of your Dell SonicWALL SMA/SRA appliance configuration settings to your local machine. The Export Settings feature 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 and export them to a file on your local management station, click the **Export Settings** button on the **System > Settings** page and save the settings file to your local computer. The default settings file is named `sslvpnSettings.zip`.

i **TIP:** To more easily restore settings in the future, rename the .zip file to include the version of the Dell SonicWALL SMA/SRA 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 Dell SonicWALL SMA/SRA appliance and then reboot the appliance with the new firmware. This procedure applies to the SMA 500v Virtual Appliance as well as the hardware appliances.

i **NOTE:** Dell SonicWALL SMA/SRA 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.

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 the **Upload** button.
 - 3 Click **OK**. The upload process can take up to one minute.
 - 4 When the upload is complete, you are ready to reboot your Dell SonicWALL SMA/SRA appliance with the new Secure Mobile Access image. Do one of the following:
 - To reboot the image with current preferences, click the boot icon for **New Firmware**.
 - To reboot the image with factory default settings, click the boot icon for **New Firmware** and select the **Boot with factory default settings** check box.
- i** **NOTE:** Be sure to save a backup of your current configuration settings to your local computer before rebooting the Dell SonicWALL SMA/SRA appliance with factory default settings, as described in the [Exporting a copy of your configuration settings](#) section.
- 5 A warning message dialog is displayed saying *Are you sure you wish to boot this firmware?* Click **Boot** to proceed. After clicking **Boot**, do not power off the device while the image is being uploaded to the flash memory.
 - 6 After your SMA/SRA appliance successfully restarts with the new firmware, the login screen is displayed. The updated firmware information is displayed on the **System > Settings** page.

Resetting the SMA/SRA appliance using SafeMode

If you are unable to connect to the Dell SonicWALL SMA/SRA appliance 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.

To reset the SMA/SRA appliance in SafeMode:

- 1 Connect your management station to a LAN port on the Dell SonicWALL SMA/SRA 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.

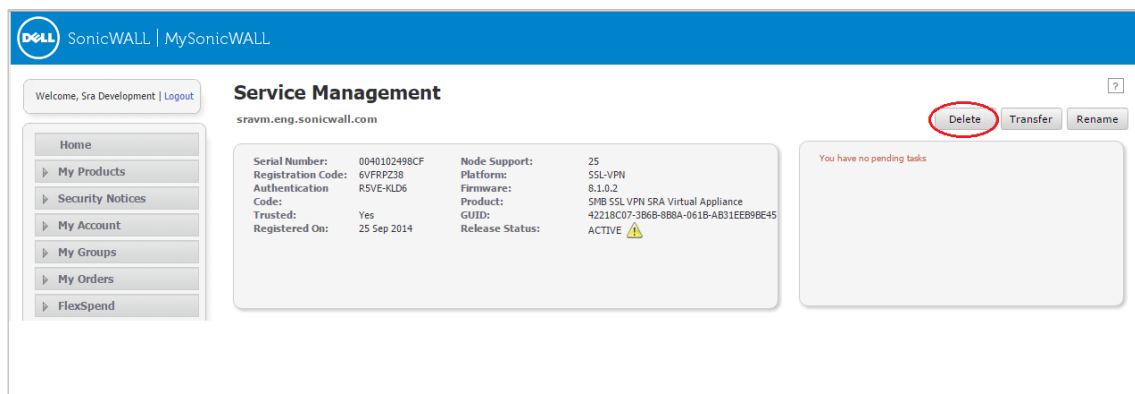
i **NOTE:** The Dell SonicWALL SMA/SRA appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.
- 2 Use a narrow, straight object, like a straightened paper clip or a pen tip, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is on the front panel in a small hole to the right of the USB connectors.

i **TIP:** If this procedure does not work while the power is on, turn the unit off and on while holding the Reset button until the Test light starts blinking.
- 3 Connect to the 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 Dell SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.
- 5 After the Dell SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset 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** check box.

Moving an SRA Virtual Appliance to SMA 8.5.0.4

An SRA Virtual Appliance running SMA 8.1 or older, cannot be upgraded to SMA 8.5.0.4 because of operating system changes in the SMA 500v Virtual Appliance software. Instead, you must reconfigure the virtual machine, as explained in the following steps:

- 1 Export the configuration settings from the old virtual appliance, as explained in [Exporting a copy of your configuration settings](#).
- 2 Make a note of the serial number and authentication code of the old virtual appliance. You can find these on the **System > Status** page.
- 3 Shut down and power off the old virtual appliance.
- 4 In MySonicWALL, click **Downloads** to open the **Download Center** page.
- 5 In the **Software Type** drop-down list, select **SMA 500v Virtual Appliance**.
- 6 In the results table, click the **SMA 500v Virtual Appliance** link to download the OVA file and save it to your local machine.
- 7 Deploy a new SMA 500v Virtual Appliance using the SMA 8.5.0.4 OVA file downloaded from <http://www.mysonicwall.com>.
- 8 Power on the new SMA 500v Virtual Appliance and configure the X0 interface using the command line interface (CLI).
- 9 Log in to the new SMA 500v Virtual Appliance as “admin” and import your saved configuration settings.
- 10 In MySonicWALL, click the serial number of the old SRA Virtual Appliance. On the Service Management page for it, click **Delete** to delete licensing for the old virtual appliance. If you are unable to delete the licensing, contact Dell SonicWALL support.



- 11 Register the new SMA 500v Virtual Appliance from the **System > Licenses** page. Enter the serial number and authentication code.

This transfers all the licensed services from the old SRA Virtual Appliance to the new SMA 500v Virtual Appliance.

To update the firmware on your new SMA 500v Virtual Appliance:

- 1 In MySonicWALL on the Download Center page, select **SMA 500v Firmware** in the **Software Type** drop-down list.
- 2 Click the desired firmware link and save the `.sig` file to your local computer.
- 3 Log into your SMA 500v Virtual Appliance, and navigate to the **System > Settings** page.
- 4 Select **Upload New Firmware** and browse to the location where you saved the firmware image file, Select the file, and click the Upload button.
- 5 Do one of the following:
 - To boot the new firmware with current configuration settings, click the boot icon for **New Firmware**.

- To boot the new firmware with factory default settings, click the boot icon for **New Firmware** and select **Boot with factory default settings**.

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

For sales or other inquiries, visit <http://software.dell.com/company/contact-us.aspx> or call 1-949-754-8000.

Technical support resources

Technical support is available to those who have purchased Dell software with a valid maintenance contract and to those who have trial versions.

Dell SonicWALL Administration Guides and related documents are available on the Dell Software Support site at <https://support.software.dell.com/release-notes-product-select>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://software.dell.com/support/>.

The site enables you to:


- View Knowledge Base articles at: <https://support.software.dell.com/kb-product-select>
- View instructional videos at: <https://support.software.dell.com/videos-product-select>
- Engage in community discussions
- Create, update, and manage Service Requests (cases)
- Obtain product notifications


Copyright 2016 Dell Inc. All rights reserved.


This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and SonicWALL are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

For more information, go to <http://software.dell.com/legal/>.

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

Last updated: 12/22/2016

232-003791-00 Rev A