



Dell SonicWALL™ Secure Mobile Access 8.5

Release Notes

June 2016

These release notes provide information about the Dell SonicWALL™ Secure Mobile Access 8.5 release.

- [About Secure Mobile Access 8.5](#)
- [Supported platforms](#)
- [New features](#)
- [Resolved issues](#)
- [Known Issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

About Secure Mobile Access 8.5

Secure Mobile Access (SMA) 8.5 is a feature release 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 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.

i **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.

New features

This section describes the new features in the SMA 8.5 release.

- [Personal Device Authorization](#)
- [RDP-HTML5 enhancements](#)
- [VNC HTML5 enhancements](#)
- [SSH and Telnet HTML5 enhancements](#)
- [Exchange Portal](#)
- [Dell SonicWALL SMA Connect Agent](#)
- [Bookmark Enhancements](#)
- [App Offloading Enhancements](#)
- [Citrix Enhancements](#)
- [Server Changes for the MC Client](#)
- [Enhanced Password Security and Local Database Authorization Changes](#)
- [Exporting Settings/TSR to FTP Server](#)

Personal Device Authorization

Topics:

- [Device Management > Devices](#)
- [Device Management > Settings](#)

Because Bring-Your-Own-Device (BYOD) has increased in popularity, IT experts are beginning to allow access to their networks. While the convenience is undeniable, the inherent risks that come with that kind of exposure must be managed. The Personal Device Authorization (PDA) feature is designed to help IT experts deal with this by utilizing the SMA appliance.

With the new PDA feature enabled, when a user attempts access to the secured network with an unregistered device, they must register that device and agree to the corporate and privacy policies in order to continue. Registration uses the device's unique Device ID for authorization, allowing future access unless revoked by you. You are able to configure and monitor all access.

Device Management > Devices

Our appliance obtains the client device's unique Device ID. You can view all devices, change device status, and delete unwanted devices.

All registered devices are listed in the table. The device and user information can be found together with the Device ID as shown in the following image.

User	Domain	Device ID	Request Time	Status	Statistics
max	LocalDomain	abcdefghij	Thu Jan 28 23:28:25 2016	Pending	[Details] [Close]
max	LocalDomain	W-D0W2CUE545502	Fri Jan 29 00:13:18 2016	Approved	[Details] [Close]
3	LocalDomain	1DFD4321-F69F-53B2-BAB3-BA9AB5916867	Fri Jan 29 00:23:45 2016	Approved	[Details] [Close]

More Detail

OS: OS X
 Model Identifier: MacBookPro11,3
 System Version: OS X 10.11.2 (15C50)
 Computer Name: derekyu's MacBook Pro
 Model Name: MacBook Pro

Device Management > Settings

Register Settings

Device Management > Settings [Accept] [Cancel]

Register Settings

- Enforce Device Register
 - Approve Method: Auto
 - Maximum Device per User: 5
 - Security Statement:

Your device will require a unique identifier in order to access the VPN network. This information is not shared with entities outside the corporation unless legally required. Click Accept to agree and proceed or Decline to decline.
 - Allow logins from apps without device registration capability

ActiveSync Provision Settings

Notification Settings

Status: Update Successful.

Enforce Device Register

This option is used to disable or enable the Personal Device Authorization (PDA). It is disabled by default.

Approve Method

There are two methods: **Auto** and **Manual**. 1) The **Manual** mode means that each device first registered by one user is set to the "pending" or "wait for the administrator to approve" status. 2) The **Auto** mode matches the registered devices with the device policies created by you. The device takes on the policies defined action when a policy is matched. If no matches are found, the device is set as approved by the system. The **Auto** mode can reduce your workload.

Maximum Device per User

This option limits the maximum devices each user can register.

Security Statement

This alert message appears on the client when the user logs in. You can customize this security statement.

Allow access from device without the capacity

This option applies to SMA Connect Agent devices, such as Linux/Android/iOS/Windows phones. Devices are able to access the appliance without device registration when you enable this option.

You can customize the registration settings at the domain level when this option is enabled. The domain level settings have a higher priority than the global settings.

ActiveSync Provision Settings

ActiveSync Provision Settings can be applied specifically to ActiveSync devices. Provision settings can override the settings on a backend Exchange server. Mobile devices are not able to sync when the Provision settings are not satisfied.

Notification Settings

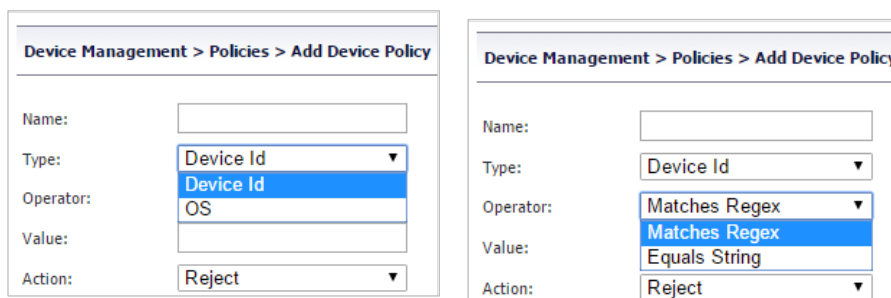
You can list a set of email addresses here. When a new registration request arrives, an email notification is sent to these addresses notifying the recipients to handle the request.

The notification email's Subject and Message can be customized.

Device Management > Policies



Device policies are applied to the situation when the approve method is set to **Auto**. This can reduce your workload.



There are two types of device policies: **Device Id** and **OS**. The **Device Id** has a higher priority than **OS** by default.

There are also two Operators: **Matches Regex** and **Equals String**. **Equals String** is case sensitive. **Equals String** has priority to **Matches Regex** by default.

The **Action** option has three choices: **Pending**, **Approve**, and **Reject**. The device takes on the defined action when it matches the policies.

Device Management > Log

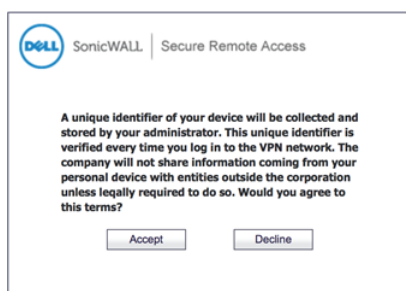
Time	Priority	Category	Source	Destination	User	Message
2020-12-12 15:45:28	Notice	Device Management	10.103.62.100	10.103.62.100	admin	Device register request from user set to Rejected
2020-12-12 15:36:04	Notice	Device Management	10.103.62.107	10.103.62.100	admin	Device register request from user set to Approved
2020-12-12 15:36:03	Notice	Device Management	10.103.62.107	10.103.62.100	System	Device Management Notification Error
2020-12-12 15:36:03	Notice	Device Management	10.103.62.107	10.103.62.100	admin	New device register request wait for approval
2020-12-12 14:57:46	Notice	Device Management	10.103.62.100	10.103.62.100	System	Device Management Notification Error
2020-12-12 14:57:46	Notice	Device Management	10.103.62.100	10.103.62.100	admin	New device register request wait for approval
2020-12-12 13:26:28	Notice	Device Management	10.103.62.100	10.103.62.100	admin	New device register request wait for approval
2020-12-12 13:26:28	Notice	Device Management	10.103.62.100	10.103.62.100	admin	Device register request from user deleted
2020-12-12 13:19:10	Notice	Device Management	10.103.62.100	10.103.62.100	System	New device register request from user approved automatically
2020-12-12 12:03:12	Notice	Device Management	10.103.62.100	10.103.62.100	admin	Device Management Log cleared

The Device management log helps you acquire additional information about your devices, including logs on new device register requests, device status changes, deleted devices, and mail notifications.

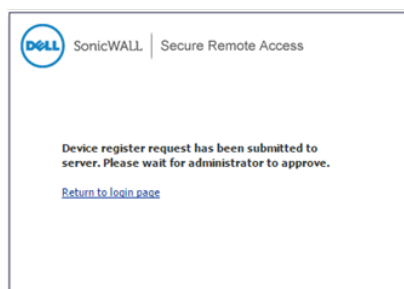
PDA for Portal Login

PDA for portal login currently is only supported in Desktop. All cases of PDA for the portal login are listed as follows:

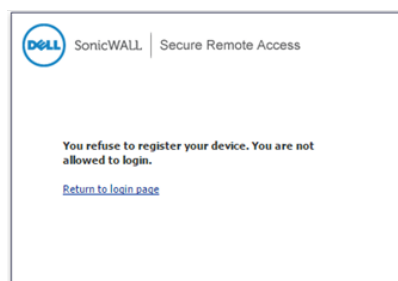
- 1 Upon first login, a security statement pops up after login authentication.



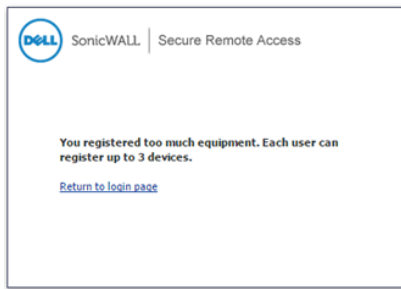
- 2 You would not be allowed access even if you accept to register your device when the device approval method is set to "Manual." You must still wait for an administrator to approve your device.



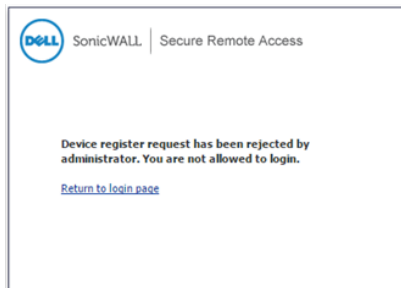
- 3 However, you would not be allowed access if you have refused to register your device.



- 4 Also, you would not be allowed to register your device or gain access for it if you had already registered three devices.



- 5 Finally, you also cannot register your device or gain access for it if your “register device” request has been rejected by the administrator.



PDA for SMA Clients

Clients including Mobile Connect, NetExtender, Virtual Assist, and Virtual Meeting are currently not supported for the PDA feature in the RTQA build (no need to support “guest login”).

Clients will be supported in a future build.

RDP-HTML5 enhancements

SMA 8.5 includes several enhancements to RDP-HTML5 bookmarks:

Topics:

- [Per-Device license support](#)
- [European keyboard support](#)
- [Copy/paste text across the RDP session](#)
- [Optimized view on tablet and phone](#)
- [RDP Feature comparison between HTML5, JAVA, and ActiveX bookmarks](#)

The license data is stored in the browser. If you use a different browser on the same device to access the same Remote Server, a new license is required.

On a Terminal Services server, you can revoke a license using the licensing manager. Only a limited number of revocations are allowed each day.

Per-Device license support

When a Remote Desktop Session Host (RD Session Host) server is configured to use the Per-Device licensing mode, and a client computer or device connects to an RD Session Host server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to an

RD Session Host server for the second time, if the Remote Desktop license server is activated and enough Remote Desktop Services (RDS) Per-Device Client Access Licenses (CALs) are available, the license server issues the client computer or device a permanent RDS Per-Device CAL. If the license server is not activated or does not have any RDS Per-Device CALs available, the device continues to use the temporary license. The temporary license is valid for 90 days.

A permanent RDS Per-Device CAL issued by a license server is configured to automatically expire after a random period between 52 and 89 days, at which time the RDS Per-Device CAL returns to the pool of available RDS Per-Device CALs on the license server.

Configuring a per-device license server

This section describes how to configure Per-Device licensing on Windows Server 2008 R2. Configuration details may vary for other server versions.

To add a license server:

- 1 In the Server Manager screen under **Edit Settings**, double-click **Remote Desktop license servers**.
- 2 In the Properties dialog, on the **Licensing** tab, click **Add**.
- 3 In the Add License Server dialog, fill in the **License server name or IP address** field and then click **Add**.

To configure the license server:

- 1 Click **Licensing Diagnosis** in the left navigation pane.
- 2 In the middle pane under **license server(s) specified**, select the desired server name or IP address. The right pane displays additional actions.
- 3 In the right pane, click **Start RD Licensing Manager**.
- 4 The next screen lists the available licenses, shown as **Temporary**.

You can manage your Per-Device license from this screen.

Every remote connection from a different web browser consumes a device license. You can revoke the license in the above screen, but only a few times in a certain period.

To install a license:

- 1 Right-click the server in the left pane under **All servers** and select **install license**, and then follow the wizard step by step. Make sure your Internet connection is available.

European keyboard support

Some European characters cannot be input on US language keyboards. The keyboard type must be set on both the Remote Server and Local Client computers.

To parse the input correctly, you need to set the same language for the HTML5 Canvas (<canvas>) element by clicking the language identifier beside the S shield to trigger the language selection menu.

S shield:



Language selection menu:



The Bookmark administrator can set the default language keyboard in the bookmark settings. When the bookmark is launched, the default language identifier is shown beside the S shield.

Copy/paste text across the RDP session

The Bookmark administrator can enable/disable this functionality in the bookmark settings with the **Redirect clipboard** option.

If enabled, after launching the bookmark and attempting to copy text on the remote server, an icon blinks below the S shield.

Click the blinking icon, and a dialog pops up with the copied text in the input field. You can copy the text manually from there and paste it to the local machine.

In the other direction, it works very smoothly just like copying/pasting locally. Simply copy the local string and paste it on remote machine.

Optimized view on tablet and phone

The following actions are supported while viewing the HTML5 Canvas on mobile devices:

- Adjust the dialog size according to screen size
- Reconnect while rotating the screen
- Control menus

RDP feature comparison between HTML5, JAVA, and ActiveX bookmarks

Feature	ActiveX	Java	Pure Java Client	HTML5
Connect and Control	Yes	Yes	Yes	Yes
TS Farm/Load Balance support	Yes	Yes	Yes	Yes
RDP 8	Yes	Yes	Yes	Yes
Wake on LAN	Yes	Yes	Yes	Yes
Console Login	Yes	Yes	No	Yes
Redirect Printers	Yes	Yes	No	No
Redirect Ports	Yes	Yes	No	No

Feature	ActiveX	Java	Pure Java Client	HTML5
Redirect Drives	Yes	Yes	No	No
Redirect SmartCards	Yes	Yes	No	No
Redirect Clipboard	Yes	Yes	No	No
Redirect PnP devices	Yes	Yes	No	No
Desktop Background	Yes	Yes	No	Yes
Dual Monitors	Yes	Yes	No	No
Span Monitors	Yes	Yes	No	No
Font smoothing	Yes	Yes	No	Yes
Remote Application	Yes	Yes	No	No
Remote Audio	Yes	Yes	No	No
Single Sign-on	Yes	Yes	Yes	Yes
Colors	up to 32 bit	up to 32 bit	up to 32 bit	up to 32 bit
Resolution	Up to 1920x1080 (set values)	Up to 1920x1080 (set values)	Up to 1920x1080 (set values)	Up to 1920x1080 (set values)
Notes	Requires Plug-in installation. Utilizes an installed mstsc client on a remote system. Loopback method (some reported issues with Windows 8)	Requires Java installed. Utilizes an installed mstsc client on a remote system. Loopback method (some reported issues with Windows 8)	Requires Java installed. Utilizes our own Java applet. Loopback method (some reported issues with Windows 8)	Requires the browser supports HTML5. Most modern browsers support HTML5. Verified on IE, Chrome, Firefox, and Safari.
Support	Windows IE only	Windows Browsers with Java (IE, FireFox, Chrome) and Mac OSX (Safari, Chrome, and FireFox)	Windows Browsers with Java (IE, FireFox, and Chrome) Mac OSX (Safari, Chrome, and FireFox) Linux (FireFox)	All devices with browsers capable of HTML5 support (Chrome, IE10+, FireFox, and Safari)

VNC-HTML5 enhancements

In the 8.5 release, the following major enhancements have been made to the VNC-HTML5 bookmarks:



Topics:

- [Performance improvement for Mac screen sharing](#)
- [Window control](#)
- [More options](#)
- [VNC feature comparison between HTML5 and JAVA bookmarks](#)

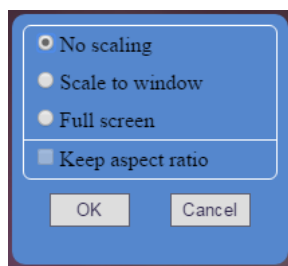
Performance improvement for Mac screen sharing

In previous releases, when a Mac was accessed through a VNC-HTML5 bookmark, the display lag was noticeable. In this release, that lag has been removed by improving the HTML5 VNC internal implementation.

Window control

In this release, the  Fit to content menu item has been replaced with the  Window menu item which provides various window controls for the VNC HTML5 client.

After the “Window” menu has been clicked, the following sub-menu appears:



In this sub-menu, several options are provided:

- **No scaling:** the picture size of the VNC HTML5 is fixed, the size of the browser’s window can be changed through user action, but when this radio button is enabled, no matter how the browser’s window has changed, the screen size of VNC remote desktop remains the same value which has been specified by the VNC server.
- **Scale to window:** the picture size of the VNC HTML5 is not fixed, and has been scaled to the size of the outside browser’s window. This means, you could change the picture size of the VNC HTML5 by changing the size of the browser’s window.
- **Full screen:** The browser will be in full screen, and the picture size of the VNC HTML5 will also be scaled to the size of the browser’s window. This option will not be shown on browsers that do not support full screen, such as Safari on iOS.
- **Keep aspect ratio:** this option is about how to scale the picture size of the VNC HTML5, and then its only available options are “Scale to window” and “Full screen.” If this radio button is enabled, the aspect ratio of the VNC HTML5 picture stays the same as specified by the VNC server; otherwise the aspect ratio of the VNC HTML5 is the same as the aspect ratio of the outside browser’s window.

More options

These enhancements are available for the SRA4600, SRA1600, SMA200, SMA400, and the SMA 500v Virtual Appliance.

The following options, which were originally supported for VNC Java, are now supported by VNC HTML5:

- 1 Encoding
- 2 Compression Level
- 3 JPEG Image Quality
- 4 Cursor Shape Updates
- 5 Use CopyRect
- 6 Restricted Colors (256 Colors)

- i** **NOTE:** 1. For the encoding options, “CoRRE” encoding is only supported by VNC JAVA.
2. Mac screen sharing does not support restricted colors, so do not enable that option if Mac screen sharing is accessed.

VNC feature comparison between HTML5 and JAVA bookmarks

Feature	HTML5 version	Java Applet version
Encoding	Yes (Not configurable, determined by the VNC server, supported encoding: Raw, Copyrect, RRE, hextile, Tight, TightPNG, and Zlib)	Yes (Can be one of Tight, Raw, RRE, CoRRE, Hextile, and Zlib)
Rotation	Yes	Not Applicable
Compression Level	No	Yes
JPEG Image Quality	No	Yes
Cursor Shape Updates	Yes (Enabled by default. Not supported on IE. For mobile browsers, "Cursor shape updates" is always disabled)	Yes
Use CopyRect	Yes (Not configurable)	Yes
Restricted Colors (256 Colors)	No	Yes
Reverse Mouse Button 2 and 3	No	Yes
View Only	Yes	Yes
Share Desktop	Yes	Yes
SSO	Yes	No

SSH and Telnet HTML5 enhancements

The following are improvements made to the HTML5 SSH and Telnet on the SRA platform. Changes apply to both SSH and Telnet HTML5 clients.

Topics:

- [SSO Support](#)
- [General Enhancements for Telnet and SSH HTML5 Terminal](#)
- [SSHv2 feature comparison between HTML5 and JAVA bookmarks](#)

Telnet and SSHv2 bookmarks are generally updated by Bookmark Unification in 8.5 releases. (For details of this update, please read “[SMA-108507 - Bookmark Enhancements \(8.5\)](#)”.)

Single Sign-On Support

Single sign-on (SSO) is supported for Telnet and SSH bookmarks. The bookmark must be configured enabling the **Automatically log in** option in the bookmark setting. If the correct username and password are set, the session is logged in automatically.

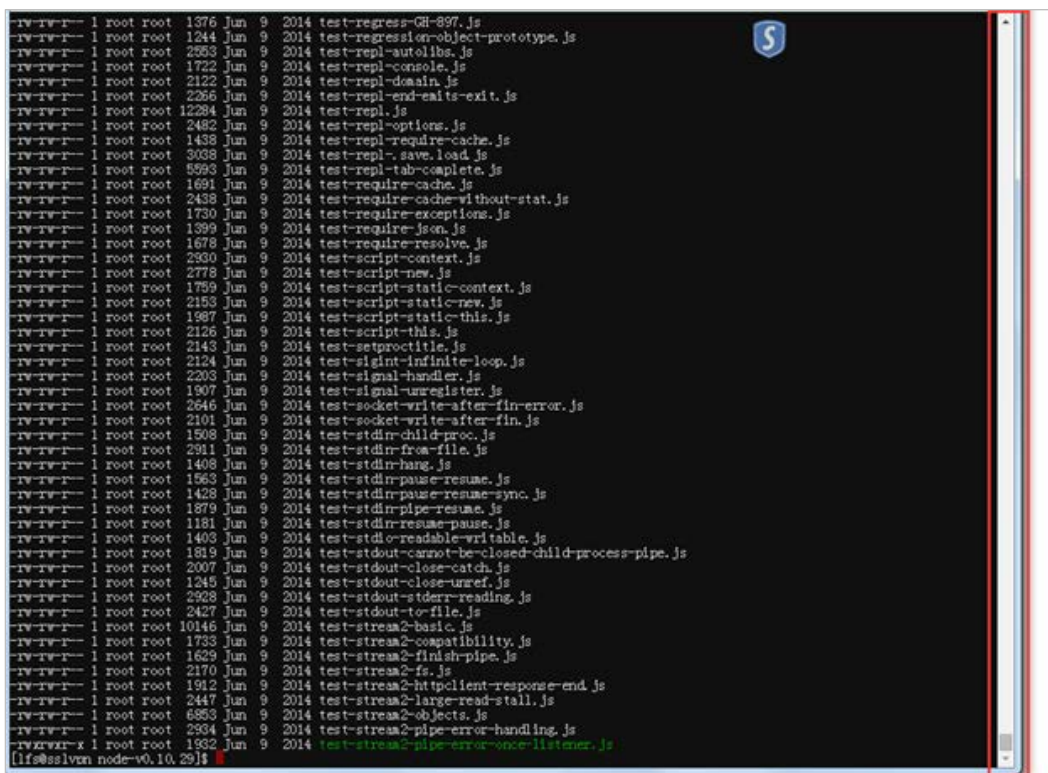
For the SSHv2 HTML5 bookmark, SSO is supported for both user name and password authentication. If SSO has failed, a menu pops-up to allow you to decide to manually fill in the credentials or cancel the log in.

General Enhancements for Telnet and SSH HTML5 Terminal

Telnet and SSHv2 HTML5 bookmarks now use a new terminal emulator. The following sections describe the primary improvements for these bookmarks.

Scrolling Back Support

The new terminal provides scrolling back support for the Telnet and SSHv2 HTML5 bookmark to view historic records. The scroll bar can also be used as text editors when appropriate for scrolling.



Dynamic Window Resize of Console Session

When the browser window is resized, the content size of the terminal emulator is changed dynamically and takes effect for the next interaction.

- Before resize



- After resize

```
[lfs@sslvpn node-v0.10.29]$ ls
AUTHORS      common.gypi  CONTRIBUTING.md  LICENSE  out      tools
benchmark    config.gypi  deps             Makefile  README.md  vcbuild.bat
BSDmakefile  config.mk    doc              node      src
ChangeLog    configure    lib              node.gyp  test
```

Copy and Paste Support

With this enhancement, you can select everything in the emulator and use OS shortcuts to copy and paste texts.

- Select the text (with blue background color) and utilize the standard copy shortcuts. When the selection disappears, the texts are copied.

```
[lfs@sslvpn node-v0.10.29]$ ls
AUTHORS      common.gypi  CONTRIBUTING.md  LICENSE  out      tools
benchmark    config.gypi  deps             Makefile  README.md  vcbuild.bat
BSDmakefile  config.mk    doc              node      src
ChangeLog    configure    lib              node.gyp  test
```

- The Paste action can be done by utilizing standard paste shortcuts.

```
[lfs@sslvpn node-v0.10.29]$ ls
AUTHORS      common.gypi  CONTRIBUTING.md  LICENSE  out      tools
benchmark    config.gypi  deps             Makefile  README.md  vcbuild.bat
BSDmakefile  config.mk    doc              node      src
ChangeLog    configure    lib              node.gyp  test
[lfs@sslvpn node-v0.10.29]$ AUTHORS
```

NOTE: For SSHv2 HTML5 bookmarks in Windows, when there are some selections, pressing Ctrl+C copies the selection. Otherwise, the '^C' signal is sent to the host.

Zoom in/Zoom out to Change Font-size

You can zoom the browser window in or out to change the font-size during runtime. Also, the content size of the terminal emulator is changed dynamically.

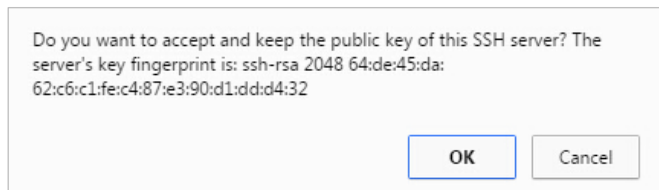
- SSHv2 HTML5 bookmark zoomed in:

```
[lfs@sslvpn node-v0.10.29]$ ls
AUTHORS      common.gypi  CONTRIBUTING.md  LICENSE  out      tools
benchmark    config.gypi  deps             Makefile  README.md  vcbuild.bat
BSDmakefile  config.mk    doc              node      src
ChangeLog    configure    lib              node.gyp  test
```

Host Key Verification and Default Font-size Option (only for SSHv2 HTML5 bookmark)

- Host Key Verification:

In the 8.5 release, host key verification is improved by completely showing the algorithm, host key length, and the host key fingerprint after first launching the SSHv2 HTML5 bookmark. You can accept or reject the verification. If you accept it, the fingerprint would be stored to the local storage of the browser. For now, the SSHv2 HTML5 bookmark only supports the 'ssh-rsa' public key algorithm.



i **NOTE:** Even if SSO is enabled, you still need to verify the host key manually before the automatic authentication can be done. (If the Automatically accept host key is not enabled.)

- Default Font-Size

A new option is now available for SSHv2 HTML5 bookmark to set the default font-size. The range of the font-size is 12 ~ 99.



SSHv2 feature comparison between HTML5 and JAVA bookmarks

Feature	HTML5 version	Java Applet version
Automatically Accept Host Key	Yes	Yes
Public/Private Keys		
Authentication	No	Yes
Bypass Username	No	Yes
Adjustable Window Size	No (Fixed window size in option)	Yes
Log Session	No	Yes
Scroll-back	No	Yes
Clipboard	No	Yes
Highlight	No	Yes
Color Options	No	Yes
Store Accepted Host Key	Yes	No
SSO	Yes	No

Exchange Portal

Application Offloading supports ActiveSync, Outlook Anywhere, Autodiscover, and OWA with one single portal. With the Exchange server as its backend server, the exchange portal has many specific settings. The Exchange Portal Wizard provides a convenient way to create the Exchange portal, and many specific options are configured automatically.

Topics:

- [Creating the Exchange Portal](#)
- [Editing the Exchange Portal](#)

Creating the Exchange Portal

Step 1. Type

The wizard starts by clicking **Offload Web Application...** on the **Portal > Portals** page.

The first tab allows you to select a portal type. If "General" or "Load Balancing" is selected, one more option is displayed that reads, "This is an Exchange Portal which will be accessed by OWA, ActiveSync or Outlook Anywhere."

Enable the option and click "Next."

Step 2. Server

The second step is called "Server" which includes the Portal and Exchange Server settings.

Portal Name - The portal name should be unique to the identity of different portals.

Portal Domain Name - Enter the domain name used to access the offloading portal.

Portal Interface - indicates which network interface the portal will be bind to. If one specific network interface is selected, a new IP address should be assigned to the portal.

Portal Certificate - Lists all certificates that have been imported.

Exchange Server Address - Accepts settings about the Exchange Server, which can simply be the IP address of the Exchange Server. The scheme of the address is "https" by default. Port and default paths can also be set in this single field.

All these settings are verified instantly from the appliance when the mouse leaves the input textbox. The reason why the input fails appears. Only when all fields are satisfied, can you click "Next" to go to the third tab.

Step 3. Security

The third step includes the Security settings.

Allowed access method - Lists the methods that the portal has accessed, including "ActiveSync," "Outlook Anywhere," and "Outlook Web Access." If one of these methods is disabled, one access policy is automatically generated to block that kind of access.

Enforce ActiveSync Provision - Provides a portal level option to enable or disable the ActiveSync Provision Settings. For more information about the "ActiveSync Provision," See Device Management (or the PDA feature).

Enable Web Application Firewall - Can be enabled when WAF is licensed.

Disable Authentication Control - Cannot be enabled for the Exchange Portal.

Step 4. Miscellaneous

The fourth step includes the general portal settings.

The default values of **Portal Site Title**, **Portal Banner Title**, and **Login Message** are designed specifically for the Exchange Portal. They can also be customized.

Editing the Exchange Portal

All Exchange Portal settings can be viewed or edited by clicking **Edit** on portal list page.

On the **General** tab, “**Enforce login uniqueness**” is disabled by default, because ActiveSync or Outlook Anywhere client may not only use one session.

On the **Offloading** tab, “**Enable Email Clients Authentication**” is enabled if “**Disable Authentication Control**” is not selected. The “**Default Domain Name**” is set automatically when creating or editing a Domain.

On the **Virtual Host** tab, “**Virtual Host Alias**” is set to the Autodiscover address of ActiveSync if ActiveSync access has been enabled. The Autodiscover address is generated automatically from the Virtual Host Domain Name.

On the **Logo** tab, a Logo or Favicon can be customized for OWA access.

On the **Services > Policies** page, one or more policy can be added to deny a specific access method that was selected during the wizard.

Dell SonicWALL SMA Connect Agent

The Browser Plug-ins (NPAPI, ActiveX, and Java Applet) are used to launch native applications such as Net-Extender, Virtual Assist EPC, and so on. For security reasons, popular browsers block these Plug-ins. The Chrome browser, for example, has disabled all NPAPI Plug-ins, and the newest Microsoft Edge browser does not support ActiveX. As such, the ease-of-use ability of launching directly from the browser is no longer functional, and a new method for seamless launching is necessary.

There is another application to launch that will open a specific Scheme URL. There are some Schemes already defined in the Windows/OS X, such as mailto. The SMA Connect Agent is a new feature to use the Scheme URL to replace the Browser Plug-ins. The SMA Connect Agent is just like a bridge to receive the Scheme URL request and launch the specific native application.

Topics:

- [Supported Operating Systems](#)
- [Downloading and Installation](#)
- [Setup](#)

Supported Operating Systems

The SMA Connect Agent supports Windows (7, 8, and 10) as well as the Macintosh (OS X) operating systems.

Downloading and Installation

On the Welcome page, the download and install notification displays when the user needs to use the EPC or PDA features:

On the Portal page, the download and install notification displays when the user attempts to launch Net-Extender, Virtual Assist, Virtual Meeting, RDP Bookmark (Native), or Citrix Bookmark (Native):

Download - the Browser downloads the SMA Connect Agent Installer.

Installed - the notification does not appear again.

Continue - closes the notification and continues the action.

[Details] - opens a window to introduce the SMA Connect Agent.

After the download is complete, it includes the Installer. The Windows installer is **SMAConnectAgent.msi**, the Macintosh installer is **SMAConnectAgent.dmg**. The Windows installer needs your permission to install, the Macintosh installer guides you to put the SMA Connect Agent to the /Application directory.

Setup

Proxy Configuration

The SMA Connect Agent can setup the proxy by user.

There are four options to setup the proxy configuration:

Log

There is a Log tray on the system toolbar. You can right-click the tray and select the popup menu to view the logs.

Browser Warning

When the Scheme URL tries to launch the SMA Connect Agent, the browser could popup a warning message to confirm that you want to launch the SMA Connect Agent:

With a Firefox warning window, press **OK** to launch the SMA Connect Agent.

In a Chrome warning window, press **Launch Application** to launch the SMA Connect Agent.

In an Internet Explorer warning window, press **Allow** to launch the SMA Connect Agent.

End Point Control

The SMA Connect Agent supports doing an End Point Control (EPC) check from the browser. If you enable the EPC check in the login page, the browser launches the specific Scheme URL requesting the SMA Connect Agent do the EPC check.

The SMA Connect Agent checks the EPC Service on the machine. If the EPC Service is not on the local machine or if there is a newer version on the Appliance, the SMA Connect Agent downloads/installs or upgrades the EPC Service. After installing or upgrading, the SMA Connect Agent does the EPC check.

If the EPC feature (Appliance side) enables the "Show EPC failed message in detail at client side," the SMA Connect Agent records the detailed fail message in the log. Then, you can view the tray Log.

Personal Device Authorization

Personal Device Authorization (PDA) is a new feature. The SMA Connect Agent helps the PDA feature get the local machine's information. In the login page, if the user enables the PDA feature, the browser launches the SMA Connect Agent. SMA Connect gets the information of the local machine and sends the information to the appliance.

SonicWALL Application

On the portal page, there are buttons you can click to launch supported SonicWALL Applications, including Net-Extender, Virtual Assist, and Virtual Meeting.



Net-Extender cannot run on Macintosh. Therefore, the SMA Connect Agent does not support the Net-Extender connection on Macintosh.

Remote Desktop Protocol Bookmark - Native

Introduced in this release is a new feature, Bookmark auto detection. For the SMA Connect Agent, there is also a new Remote Desktop Protocol (RDP) type that has been added into the RDP Bookmark - **Native**.

If you select "Native" to launch the RDP bookmark, then the SMA Connect Agent launches the RDP Client on the local machine to do the RDP connection.

Windows:

The SMA Connect Agent launches the "mstsc.exe" executable to complete the RDP connection.

Macintosh:

The SMA Connect Agent searches for the "Microsoft Remote Desktop" App. The SMA Connect Agent launches the "Microsoft Remote Desktop" to do the RDP connection. If you have not yet installed the App, the SMA Connect Agent pops up the App's web page for installing it. So far, the SMA Connect Agent on Macintosh cannot support the SSO.

Citrix Bookmark - Native

If you select "Native" to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection.

Windows:

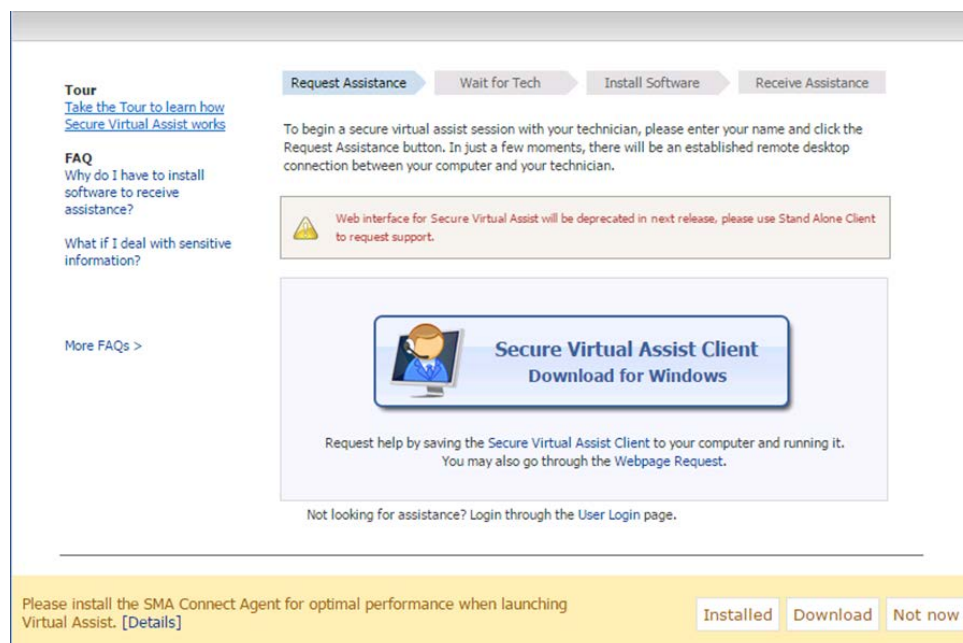
The SMA Connect Agent tries to open the ICA file to launch the Citrix Receiver. If the Citrix Receiver is not installed, the system pops up a message.

Macintosh:

The SMA Connect Agent searches for the "Citrix Receiver" App; to be sure you have installed the App. The SMA Connect Agent launches the "Citrix Receiver" to make the Citrix connection. If you have not yet installed the App, the SMA Connect Agent pops up an alert message for you to start the installation.

Direct Interface

You can access three interfaces by accessing the URL: supportLogin, vmLogin, and vmLoginCreator. The SMA Connect Agent replaces the Active-X and Java-Applet on these pages to launch the Virtual Assist and Virtual Meeting (on Windows and Macintosh). There is a notification button bar on the pages for you to install the SMA Connect Agent.



Bookmark Enhancements

This release includes new framework, Bookmark Unification, which includes the following unified bookmarks:

- Remoter Desktop Protocol (RDP) Bookmark
- Virtual Network Computing (VNC) Bookmark
- Citrix Bookmark
- Telnet Bookmark
- SSHv2 Bookmark

Topics:

- [Access Type Selection](#)
- [Unified Bookmarks](#)
- [Upgrade Conversion](#)

Access Type Selection

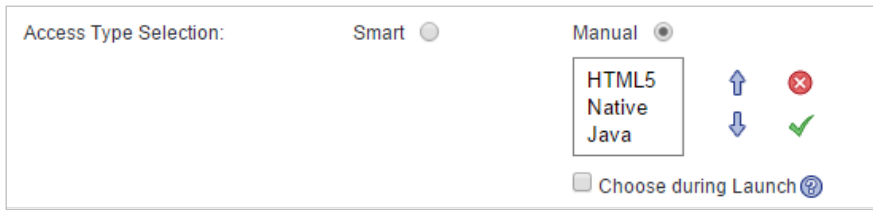
In the 8.5 release, when you try to create or edit one of the unified bookmarks, a new option, **Access Type Selection**, is provided.

- **Smart**: allows the firmware to decide which mode to launch on the client.



When creating a new unified bookmark, **Smart** is selected by default. Auto-detection is processed using bookmark-specific default modes while launching the bookmark.

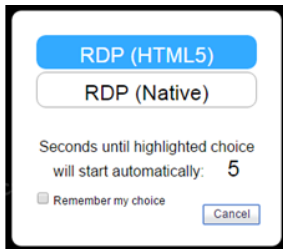
- **Manual:** provides options to configure the modes, their priorities, and the choose method. At least one mode should be enabled in the selection box.



Up and down arrows are used to adjust the launch priority. Fork and tick are used to disable or enable the modes. Disabled modes are put at the bottom of the list with a gray font color.

The **Choose during Launch** option is not enabled by default under the **Manual** mode. In this setting, while launching the bookmark, the first available mode in the configured list is run at once after auto-detection.

After the **Choose during Launch** option is enabled, while launching the unified bookmark, if there are multiple modes available for the client, a menu is provided from which you can choose within a five second count-down. When only one mode is available, the bookmark is also run immediately.



If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

That means, when next launching the bookmark, the remembered mode is run directly within two seconds. Clicking anywhere in the HTML can 'forget' the remembered mode so you can re-choose.

Editing or deleting the bookmark in the same browser can also reset the remembered mode.

If no mode is able to run on the client with the configuration, the following notice appears.

Unified Bookmarks

This section describes options for unified bookmarks and shows the default launch modes of them.

Unified Options

Options for unified bookmarks are also combined on the same edit page. For the bookmark with complex options (like RDP), options are mixed from all the modes and distinguished with tips like ***non-html5**, or ***for html5**.



For the other bookmarks like VNC and SSHv2, the options are divided into specific mode settings and common settings.

The screenshot shows a dialog box titled "SSHv2 Java Settings". It has a "Show Options" button at the top left. Below it, there are three sections: "SSHv2 HTML5 Settings" with a "Default Font Size" input field set to "15"; "Automatically log in" with an unchecked checkbox; and "SSHv2 Common Settings" with two unchecked checkboxes: "Automatically accept host key" and "Display Bookmark to Mobile Connect clients".

Default Launch Modes

The default launch modes can also be viewed by looking over the selection when creating a new unified bookmark and selecting **Manual**.

- RDP Bookmark
HTML5, Native, Java
- VNC Bookmark
HTML5, Java
- Citrix Bookmark
HTML5, Native, ActiveX
- Telnet Bookmark
HTML5, Java
- SSHv2 Bookmark
HTML5, Java

Upgrade Conversion

When upgrading to the 8.5 release, the old bookmarks are converted to the unified service type with the **Manual** settings selected and the original mode being set to the highest priority and **Choose during Launch** not enabled. You are not notified of the changes when launching the bookmark.

For example, an old SSHv2 Java bookmark is converted to the following configuration:

The screenshot shows a dialog box titled "Access Type Selection". It has two radio buttons: "Smart" (unchecked) and "Manual" (checked). Below the radio buttons is a list box containing "Java" and "HTML5". To the right of the list box are four icons: an up arrow, a down arrow, a red 'X', and a green checkmark. At the bottom, there is a checkbox labeled "Choose during Launch" which is unchecked.

App Offloading Enhancements

The current App Offloading portal creation process is not easy to use if you are unfamiliar with it. The App Offloading Portal Wizard is designed to make the creation of the App Offloading portal easier to follow. The Wizard leads you through the creation step-by-step and your inputs are instantly verified by the backend server. Many options are hidden and are set to default values. After the portal is created, all options can still be fine-tuned through the editing portal.

Topics:

- [Creating an App Offloading Portal](#)
- [Edit App Offloading Portal](#)
- [Authentication Controls enhancement](#)
- [Other App Offloading Enhancements](#)

Creating an App Offloading Portal

Step 1. App Offloading Portal Type

Start the wizard by clicking **Offload Web Application ...** on the **Portal > Portals** page. The first tab allows you to select the portal type.

Portals > Portals > Offloading Portal Wizard

1. Type 2. Server 3. Security 4. Miscellaneous

Please specify the Application Offloading Portal type:

- General
- Load Balancing
- URL Based Aliasing
- This is an Exchange Portal which will be accessed by OWA, ActiveSync or Outlook Anywhere

Previous Next

General - can be selected for most scenarios.

Load Balancing - is used to setup a Load Balancing Offloading portal.

URL Based Aliasing - is used to setup a URL Based Aliasing Offloading portal.

The Exchange portal option is designed for use with the Exchange Portal.

Step 2. Generic Server Settings

When **General** is selected, the second step appears as follows. The Portal and Application Server settings can be set on this page.

Portal Name - should be a unique name to identify different portals.

Portal Domain Name - this is the domain name used to access the offloading portal.

Portal Interface - indicates which network interface the portal is bound to. If one specific network interface is selected, a new IP address is assigned to the portal.

Portal Certificate - lists all certificates that have been imported.

Application Server Address - accepts settings about the Application Server. It can simply be the IP address of the Application Server. The scheme of the address is "https" by default. The port and default path can also be set in this single field.

All these settings are verified instantly from the Appliance when the mouse leaves the input textbox. If the input fails, the reason it failed is shown. Only when all fields are satisfied, can you click **Next** to go to the next tab.

Step 2 (alt). Load Balancing Server Settings

When **Load Balancing** is selected, the Server page appears as follows.

Load Balancing Group - replaces **Application Server Address** to show the existing Load Balancing Group to which you can assign to this portal. If no Load Balancing Group exists, you can create a new one by clicking "click here to create."

Step 2 (alt). URL Based Aliasing Server Settings

If **URL Based Aliasing** is selected, the Server step appears as follows.

Existing **URL Based Aliasing Group** is listed to assign to this portal. If no URL Based Aliasing Group exists, you can create a new one by clicking the hyperlink.

Step 3. Security Settings

The third step is for the **Security** settings including **Enable Web Application Firewall** and **Disable Authentication Controls**.

If WAF is licensed, both options can be set. If WAF is not licensed, both options are hidden.

Step 4. Miscellaneous Settings

The fourth step includes general portal settings.

Portal Site Title, **Portal Banner Title**, and **Login Message** are set by default. But they can still be customized.

Restart Now - Gracefully restarts the appliance immediately after clicking **Finish**.

More advanced options can be fine-tuned by editing this portal after the wizard is finished. Changing the Portal settings requires a web server restart that could disconnect any active NetExtender connections and certain Bookmarks. If you want to proceed with restarting the web server for the settings to take effect immediately, check **Restart now**. Otherwise, uncheck the checkbox to save the changes without web server restarting. You can restart the appliance later from the **System > Restart** page.

The wizard ends after clicking **Finish**. The page is blocked and you are redirected to the portal list page after the App Offloading portal is successfully created.

Edit App Offloading Portal

All App Offloading Portal settings can be viewed or edited by clicking the **Edit** icon on portal list page.

Authentication Controls enhancement

The enhancement disables anonymous access to the application offloading portal under two conditions; when WAF is not licensed or when accessing the Exchange portal.

If the Authentication Controls are already disabled and WAF is not licensed, after upgrading to 8.5, an **Action Required** message is shown on the portal page. **Disable Authentication Controls** is also disabled. Click **Save** to finalize the Authentication Controls setting.

If the end user accesses the portal in this condition, an error message displays.

Error: Anonymous access not allowed because Web Application Firewall is not licensed. Please contact your administrator.

A log message is generated at the Notice level that reads; *Anonymous Offloaded Connection could not be processed because WAF is not licensed. Activate the WAF subscription service or Free Trial from the System > Licenses page.*

The same is true for the Exchange portal access if **Authentication Controls** is disabled.

The log message reads, "Anonymous Exchange access could not be processed, please enable Authentication Controls for the portal."

Other App Offloading Enhancements

One new option named "Proxy Host" is added to provide the ability to select which host name is sent to the backend server.

Portals > Portals > Edit Portal: sales

General Offloading

Application Offloader Settings

Enable Load Balancing

Enable URL Based Aliasing

Enable URL Rewriting for self-referenced URLs

Scheme: Secure Web (HTTPS)

Application Server Host: 10.103.227.20

Application Server IPv6 Address:

Port Number (optional):

Homepage URI (optional):

Proxy Host: Inherited from client request

Inherited from client request

Virtual Hostname

Application Server Host (backend)

Security Settings

Options include **Inherited from client request**, **Virtual Hostname**, and **Application Server Host (backend)**. **Inherited from client request** is the default value.

Citrix Enhancements

Citrix bookmarks are generally updated with Bookmark Unification in the 8.5 release. (For details of this update, please read [SMA-108507 - Bookmark Enhancements \(8.5\)](#)).

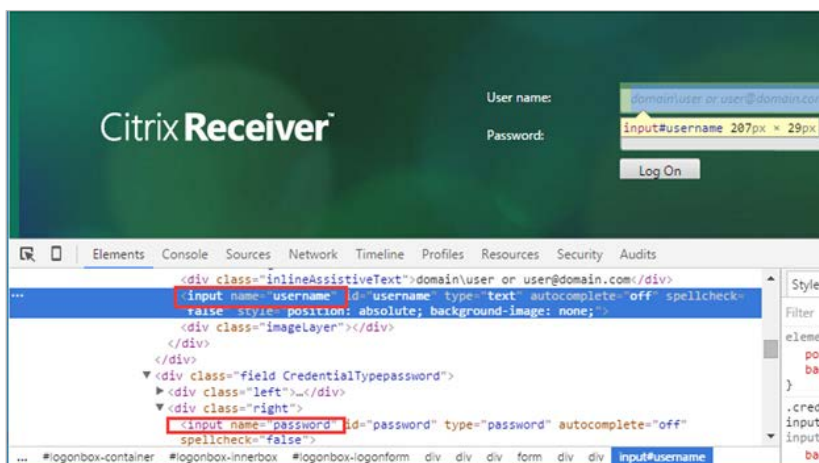
Topics:

- [SSO Support](#)
- [StoreFront 3.0.x Support](#)
- [Citrix Native Bookmark Support](#)

SSO Support

Single sign-on support for Citrix bookmark provides **Forms-based Authentication** to automatically log in the StoreFront portal that uses the **User name and password** authentication method. Complete the following to enable SSO:

- Visit the StoreFront portal directly or through the Citrix bookmark. Find the name attributes of the user and password form fields. (Usually they are **username** and **password** by default.)

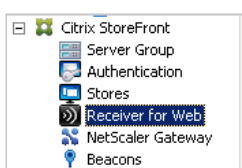


- Enable **Automatically log in** for the Citrix bookmark. Only **Forms-based Authentication** can be used for Citrix bookmark SSO. Select or fill in the credentials, including the **User Form Field** and the **Password Form Field**.
- After launching the Citrix bookmark, you can automatically log in to the StoreFront portal as shown in the following image and it is ready to use the XenApp or XenDesktop.

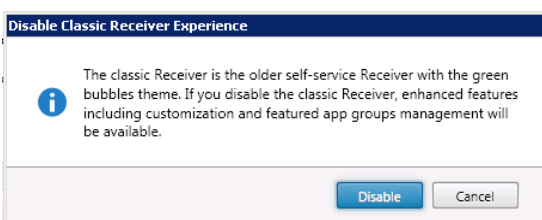
StoreFront 3.0.x Support

This section describes the StoreFront 3.0.x support with the **Classic Receiver Experience** disabled.

- Launch *Citrix Studio* or *Citrix StoreFront* on the Citrix server
- Choose **Receiver for Web**




- Click **Disable Classic Receiver Experience** to disable it. The StoreFront is then set to the **non-classic experience**.



- Launch the Citrix bookmark to experience the **non-classic experience** StoreFront.

Citrix Native Bookmark Support

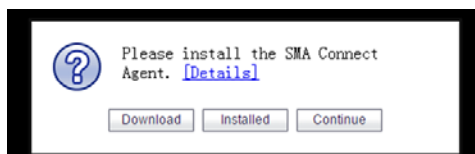
In the 8.5 release, the Citrix Native Bookmark is supported and it can provide advanced features when launched on Windows and OS X platforms after installing the SMA Connect Agent and Citrix Receiver.

 **NOTE:** For more information about the SMA Connect Agent, read [Dell SonicWALL SMA Connect Agent](#).


SMA Connect Agent

To launch Citrix Receiver through Citrix bookmark, you must first install the SMA Connect Agent.

Launch the Citrix native bookmark. If the SMA Connect Agent is not installed, the following message appears:



Click **Download** to download and install SMA Connect Agent. After that, users can click **Installed** to tell the browser to 'remember' that the SMA Connect Agent has been installed, or click **Continue** just to bypass the page and log in to the StoreFront.

 **NOTE:** For more information about the SMA Connect Agent, read [Dell SonicWALL SMA Connect Agent](#).

Launch Citrix Native Bookmark


After logging in to the StoreFront, launch any Citrix desktops or applications such as other Citrix bookmarks. A browser confirmation message might appear.

Click **Launch Application** and the Citrix Receiver launches automatically.

Launch Modes Updates

The default launch modes of the Citrix bookmarks have been converted to **HTML5**, **Native**, **ActiveX**.

Meanwhile, the Citrix Java bookmarks have been removed, and the original Citrix Java bookmarks are replaced with Citrix native bookmarks.

 **NOTE:** The Resource Window Size option is only for Citrix ActiveX bookmarks after they are upgraded because the Citrix native client (Citrix Receiver) supports dynamic window resizing and full-screen mode with its own switch.

Server Changes for the MC Client

With the SMA 8.5 release, several changes were made to accommodate the Mobile Connect 4.0 and planned 5.0 features. Changes include modifications to the Admin settings regarding TouchID, Fingerprint Authentication, as well as changes to in-app secure web browsing for SSO support.

Changes include authentication using the fingerprint technology known as TouchID on iOS or Fingerprint Authentication on Android devices. These settings either allow or disallow clients to utilize the feature when authenticating to the SMA devices. These settings also allow you to determine and allow the feature based on your requirements, and should vulnerabilities be discovered, enable you to disable the feature without additional updates.

For the planned MC 5.0 in-app web browser feature, SMA now includes a method to securely pass SSO information to the client. SMA includes a server-side implementation to support this feature along with the bookmark settings to enable to disable it.

Topics:

- [Authenticating with Fingerprint](#)

Authenticating with Fingerprint

To allow or disallow Authentication with Fingerprint, you must configure the feature in the NetExtender Settings section. Configuration is allowed globally, by group, or per user.

The control only blocks future attempts to log in with fingerprint technology when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection, so in some cases, a client might not be conforming to previous policies for the initial connection.

Enhanced Password Security and Local Database Authorization Changes

Topics:

- [Default Expiration](#)
- [Automatic Encryption Update](#)
- [Forward Compatibility](#)

Changes were made to update the way the SMA appliance handles the storing of passwords in its database. Previously, the appliance used an MD5 hashing algorithm to store passwords; however, that method has since been determined insecure. Updates to a more secure method for storing passwords on the local file system have now been implemented.

SRA and SMA 200/400 appliances have the ability to create local users with password policies enforced. Passwords were originally stored with the SHA128 hashing and included the export of settings and TSR. A need to enhance the encryption as well as forcing the expiration of passwords was required for improved security practices. As part of Enhanced Password Security, additional changes to the Local User implementation were also required.

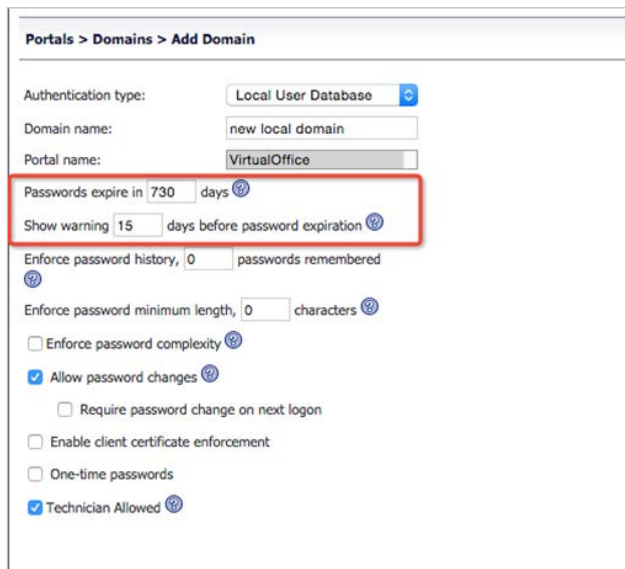
Changes to the Local Database Users include:

- 1 Default Expiration set to two years
- 2 Domain/User setting controls for Password expiration on Local DB users
- 3 Automatic update of encryption algorithm
- 4 Forward compatibility for importing of settings

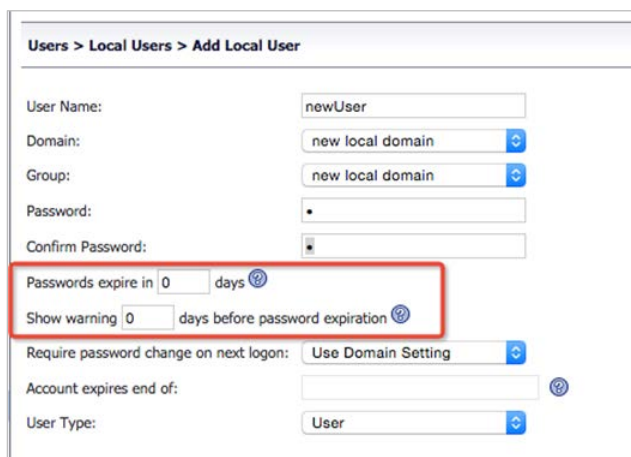
In addition to the visible changes you could set, there were other changes made to increase encryption strength.

Default Expiration

All newly created domains in the local database user type should be set with a default password expiration value, as well as the “show expiration warning days” option set to 15. You can manually change it upon creation.



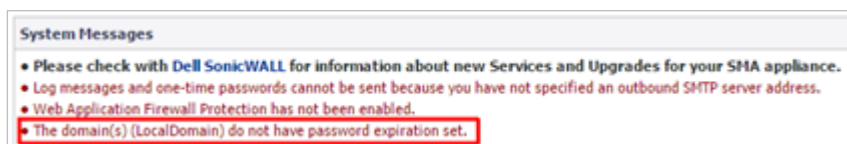
All newly-created users should also have the default password expiration value set when the domain has been set with no expiration, as well as the “show expiration warning days” option set to 15. If the domain is set with concrete password expiration days, you should also set the user expiration to 0. That means using the domain expiration setting. The domain setting detection is automatic after submitting the “adding user” request. Also, you can manually change it on creation.



The default password expiration value is two years (730 days).

On upgrade, the existing values for password expiration should remain as they are.

A notice was added in the Admin status page to recommend setting the expiration from all local database domains. The notice has a list of domains (top 5) that need that setting. If you set the default password expiration for all the domains, then the message is dismissed.



Automatic Encryption Update

After upgrading, all local db users have their password encryption updated. The process is transparent to the end user, but can be verified by examining the exported settings.

In future builds, the encryption strength automatically updates, but still requires the user to log in, as the encryption is a one-way and the login required.

Forward Compatibility

Importing settings from older firmware to 8.5 and newer firmware must support and maintain your ability, and that of other local database users, to login. As password encryption changes over time, the firmware must still allow login using the old hash at least once.

Exporting Settings/TSR to FTP Server

Currently, the running settings and logs are stored locally on the device. You can manually download them. You now have the ability to export logs to an external server, such as an FTP server.

New options have been added to automatically send the running settings and Tech Support Report (TSR) to an external FTP server. These options assist you in backing up your settings and reverting back to their working environment. Also, this helps you proactively collect diagnostic data on regular intervals, thereby giving you more control on the log collection process.

Topics:

- [System > Settings](#)
- [System > Diagnostics](#)

System > Settings

Options for automatically sending settings to the external FTP server after a firmware upgrade and upon generation are listed below. It already has a period backup of the appliance settings. These options provide a new method for backup.

Options for automatically sending the TSR to an external FTP server on restart and upon generation are listed here.

System > Diagnostics

If you want to enable the second option, notice that the Scheduled TSR would first have to be enabled on the /diag page in order to be reflected under the **System > Diagnostics** section.

Automatically sending the settings and the TSR to an external FTP server needs the required external FTP/TFTP server settings in the appliance from the **System > Administration** page in order to be properly configured.

Resolved issues

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

Security updates

Resolved issue	Issue ID
An OpenSSL Advisory from May 3, 2016 recommends upgrading OpenSSL for SMA because without the upgrade, an MITM attacker can use a padding oracle attack to decrypt traffic. Occurs when the connection uses an AES CBC cipher and the server supports AES-NI.	173618

Citrix

Resolved issue	Issue ID
Support for the native .msi and .exe Citrix clients is needed. Occurs when using the XenApp ICA client installation via .exe or .msi and trying to connect to an ActiveX Citrix link.	160838
Applications accessed by Citrix bookmarks do not launch. Occurs when using Citrix XenApp 6.5 with Java or ActiveX bookmarks with an appliance running SRA 7.5 and an out of date Citrix client.	144184

Endpoint Control

Resolved issue	Issue ID
After upgrading to EPC 8.25, it does not work correctly with Windows firewall. Occurs after upgrading the SMA firmware from 8.0.0.3 to and 8.1.0.2 and the EPC from 8.22 to 8.25.	173829

Fileshares

Resolved issue	Issue ID
Using Mobile Connect and sending a large file to the internal server, the transfer stops and the continuous pings times out. Occurs when connecting to Mobile Connect with Windows 10.	172299
CIFS HTML file share bookmark is not functioning correctly. Occurs with SMB3 & NTLMv2 support.	168521

FTP

Resolved issue	Issue ID
Uploading and downloading files via an FTP bookmark does not work and errors are displayed. Occurs after the appliance firmware is upgraded from SRA 7.5 to 8.1. The FTP bookmark points to a Linux server in which the FTP server is hosted.	167494

HTML5

Resolved issue	Issue ID
After creating a new HTML5 bookmark, cannot copy and paste text from the local client machine to a server. Occurs when trying remote to and from the RDP HTML5 bookmark.	173821

Resolved issue	Issue ID
Using the RDP HTML5 bookmark, the Move View option does not work correctly with Mobile Connect. Occurs when using user credentials in the appliance and clicking on S shield.	173623
Cannot utilize the real Chromebook keyboard for input. Occurs when using a Chromebook with a touch screen and connecting with RDP HTML5.	173620
Cannot connect to the RDP server. Occurs when the server has been set with the %AD:wWWWHomePage% custom variable (for example).	173617
HTML5 keyboard issue with many keyboard characters not working for MAC users. Occurs when using the German Switzerland MAC keyboard.	172857
The print screen key is not available. Occurs when accessing the RDP HTML5 bookmark.	172760
The French (Canadian) keyboard layout is not available. Occurs after connecting to the RDP HTML5 bookmark.	171397
The Belgian keyboard is not available. Occurs after connecting to the RDP HTML5 bookmark.	169052
The cursor/pointer does not display correctly. Occurs when using the HTML5 RDP session.	167663
After closing the session in Windows, the appliance either tries to reconnect to the servers and results in a session open/close loop, or the user cannot connect with a new session. Using the full screen display causes the session to disconnect, and also results in a session open/close loop. Occurs when clicking on an HTML5 bookmark that opens a Windows Remote Desktop Services (RDS) session. The session open/close looping occurs when the Auto Reconnection option is enabled. The inability to create a new session occurs when the Auto Reconnection option is disabled.	166869
RDP bookmarks have various issues, including not connecting to the internal servers, experiencing a reconnecting loop, and disconnecting the user after connecting. Occurs when using RDP HTML5 and RDP ActiveX bookmarks to a Windows 2012 R2 server, with RDP load balancing configured. Occurs on several browsers, including IE11, Edge, and Chrome.	165675
The ALT-TAB functionality is not working correctly. Occurs when using the HTML5 remote session.	164061
Non-English language keyboard layouts cannot be selected for an HTML5 bookmark. Occurs when configuring a bookmark and the administrator clicks on the language indicator, such as EN, beside the S-shield and attempts to select the default language and keyboard layout.	159859
Users cannot copy text from a client machine and paste it into a server or vice versa. Occurs when using an HTML5 bookmark to access the server.	154688

Log

Resolved issue	Issue ID
One Time Password logs are not being reported after successful logins. Occurs after setting up the one time passwords for users while using an internal email server with the same configuration as when it was initially deployed.	173742

NetExtender

Resolved issue	Issue ID
Unable to run NetExtender on some Windows systems. Occurs when certain Windows 7 driver updates have not been installed. See Microsoft update KB3033929 at https://www.microsoft.com/en-us/download/details.aspx?id=46148 .	175115
Using Windows 10, the Mobile Connect client coalesces multiple packets together and combines them with partial packets that SMA does not support. Occurs when using the async mode for Mobile Connect/NetExtender.	173691
Internet Explorer crashes on Windows 8.1 Pro for 64-bit systems. Occurs when uninstalling NetExtender installed with msi.	171134
Host names are not passed on with NetExtender DHCP requests. Occurs after the NetExtender client has acquired an IP address so the host name can synchronize with the DNS server.	164364

Services

Resolved issue	Issue ID
The server certificate has expired for Geo-IP filter. Occurs when trying to synchronize with the Geo-IP.	173828

WAF

Resolved issue	Issue ID
The Protection Mode option for form-based CSRF protection is not available. Occurs because the CSRF protection script is injected into offloaded portals when WAF is enabled.	173619
Unexpected URL token added. Occurs when WAF-CSRF Protection is enabled for any application offloading with external links.	173611

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

NetExtender

Known issue	Issue ID
Mobile Connect's socket connect fails after logging in to the SMA appliance. Occurs when Avast's 'Web Shield' feature is enabled.	174175

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

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	8.5.792-1
NetExtender Linux RPM 64-Bit	8.5.792-1
NetExtender Linux TGZ 32-Bit	8.5.792
NetExtender Linux TGZ 64-Bit	8.5.792

Description	Version
NetExtender MacOSX	8.5.788
NetExtender Windows	8.5.245

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.x
Virtual Assist Linux TGZ	8.5.x
Virtual Assist MacOSX	8.5.0.1
Virtual Assist Windows	8.5.0.1
Secure Virtual Meeting MacOSX	8.5.0.1
Virtual Meeting Windows	8.5.0.1

Product licensing

The Dell SonicWALL Secure Mobile Access 8.5 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](#)

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_8.5.0.0_8.5.0_p_13sv_904041.sig`
 - For the Dell SonicWALL SMA 200 appliance, this is a file such as:
`sw_sma200_eng_8.5.0.0_8.5.0_p_13sv_904041.sig`
 - For the Dell SonicWALL SRA 4600 appliance, this is a file such as:
`sw_sra4600_eng_8.5.0.0_8.5.0_p_13sv_904041.sig`
 - For the Dell SonicWALL SRA 1600 appliance, this is a file such as:
`sw_sra1600_eng_8.5.0.0_8.5.0_p_13sv_904041.sig`
 - For the Dell SonicWALL SMA 500v Virtual Appliance, this is a file such as:
`sw_smavm_eng_8.5.0.0_8.5.0_p_13sv_904041.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 **Accept** 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.

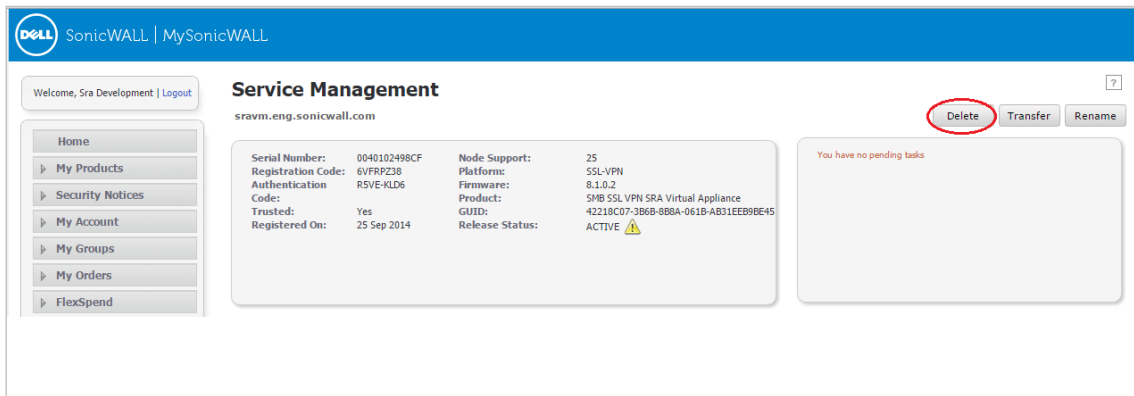
- 3 Connect to the management interface by pointing the Web browser on your management station to <http://192.168.200.1>. The SafeMode management interface displays.
- 4 Try rebooting the Dell SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current 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

An SRA Virtual Appliance running SMA 8.1 or older, cannot be upgraded to SMA 8.5 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 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.

- 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.



- 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:

- In MySonicWALL on the Download Center page, select **SMA 500v Firmware** in the **Software Type** drop-down list.
- Click the desired firmware link and save the `.sig` file to your local computer.
- Log into your SMA 500v Virtual Appliance, and navigate to the **System > Settings** page.
- Select **Upload New Firmware** and browse to the location where you saved the firmware image file, Select the file, and click the Upload button.
- 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**.

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

- Chat with a support engineer
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

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.

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.

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: 6/29/2016

232-003311-00 Rev A