Dell SonicWALL™ Secure Remote Access 8.0

Release Notes

March 2015

These release notes provide information about the Dell SonicWALL SRA 8.0 release.

About SRA 8.0

The SRA 8.0 release provides a list of new features, known issues, resolved issues, licensing information, and upgrading information.

Supported platforms

The SRA 8.0 release is supported on the following Dell SonicWALL platforms:

- Dell SonicWALL SRA 1200
- Dell SonicWALL SRA 1600
- Dell SonicWALL SRA 4200
- Dell SonicWALL SRA 4600
- Dell SonicWALL SRA Virtual Appliance

New features

The following enhancements and new features are introduced in the Dell SonicWALL SRA 8.0 release:

HTML5 RDP enhancements

The following are HTML5 RDP enhancements:

- TLS and NLA Support
- Server Verification
- Remote Application
- Audio Redirection

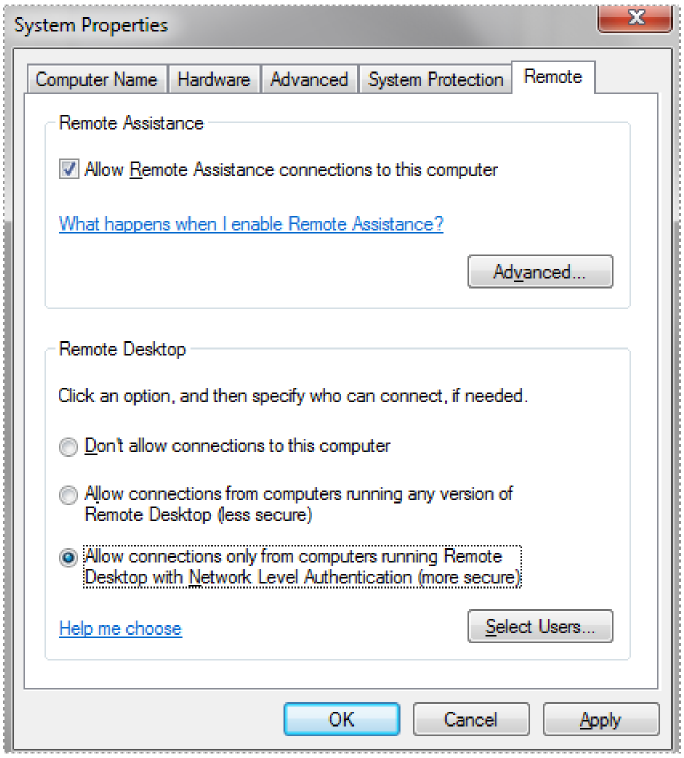
TLS and NLA

TLS and NLA are security enhancements for Remote Desktop Protocol (RDP), which now has the following three levels of security:

- Plain RDP handles encryption and decryption with the RDP protocol
- TLS bridges an SSL channel between the proxy and server
- Network Level Authentication (NLA) performs network level authentication on the basis of TLS

The security level is negotiable. TLS is enabled by default, but can be upgraded to NLA, or downgraded to Plain RDP.

You can configure the security settings on the server side from the following screen:



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

Server verification

This feature allows you to verify the server's certification whenever connected to an RDP server. The system displays a message box with the following statement:

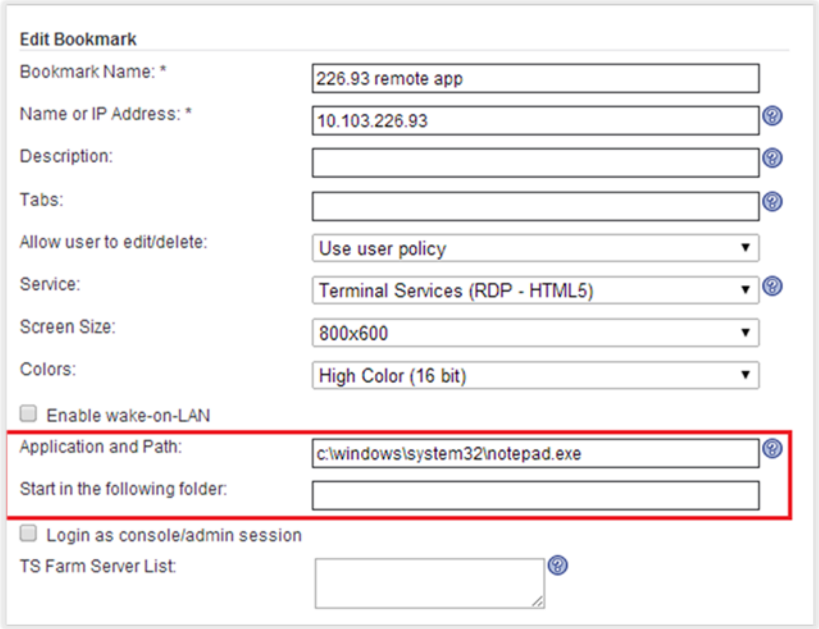
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed. Do you want to continue?

- To view the server's certificate, click the **View** button.
- To accept the certificate and launch the connection, click the **OK** button.
- To abort the connection, click the **Cancel** button.

Remote application

Remote application pops up a single application to the user instead of the whole desktop.

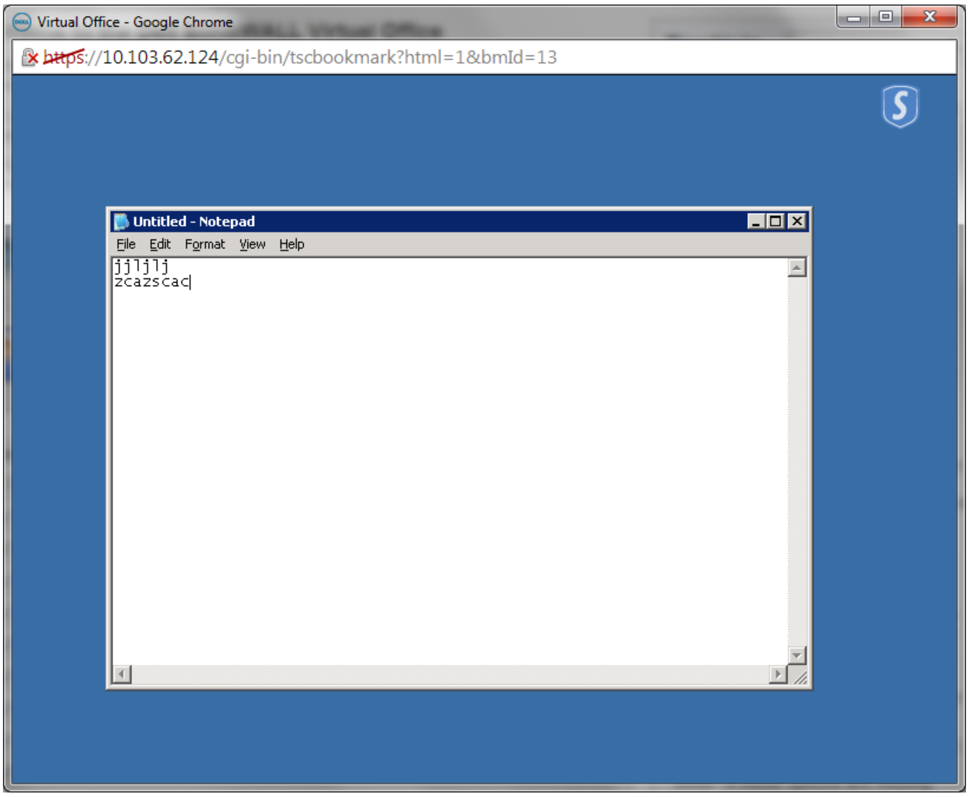
To use this feature, configure the options on your SRA management console as shown below (Services > Bookmarks > Add/Edit Bookmark).



Edit Bookmark

Bookmark Name: *	226.93 remote app
Name or IP Address: *	10.103.226.93
Description:	
Tabs:	
Allow user to edit/delete:	Use user policy
Service:	Terminal Services (RDP - HTML5)
Screen Size:	800x600
Colors:	High Color (16 bit)
□ Enable wake-on-LAN	
Application and Path:	c:\windows\system32\notepad.exe
Start in the following folder:	
□ Login as console/admin session	
TS Farm Server List:	

When properly configured, a remote application window appears as shown below:

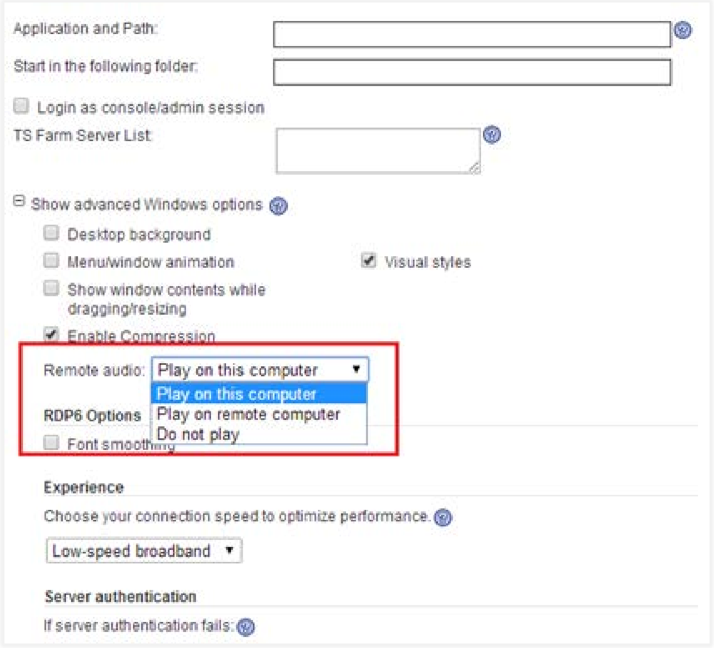


~~https~~://10.103.62.124/cgi-bin/tscbookmark?html=1&bmId=13

jjljlj
zcazscac

Audio redirection

Audio redirection enables you to play an audio clip remotely or locally. It is supported by Chrome, Firefox and Safari. You can configure the settings as shown below. On the Services > Settings > Bookmarks page, half-way down the page, click **Show Advanced Windows Options** and click the drop-down menu.



Application and Path:

Start in the following folder:

☐ Login as console/admin session

TS Farm Server List

⊟ Show advanced Windows options

☐ Desktop background

☐ Menu/window animation

☑ Visual styles

☐ Show window contents while dragging/resizing

☑ Enable Compression

Remote audio: Play on this computer

RDP6 Options

☐ Font smoothing

Experience

Choose your connection speed to optimize performance.

Low-speed broadband

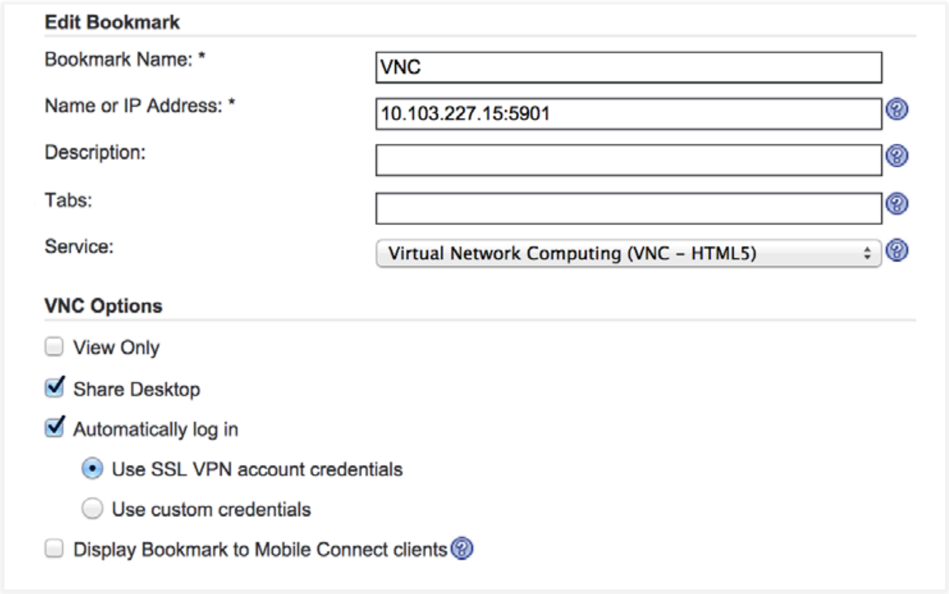
Server authentication

If server authentication fails:

- When you select **Play on this computer**, the remote audio sample is played on the client computer.
- When you select **Play on remote computer**, the remote audio sample is played on the server side.

HTML5 VNC enhancements

In SRA 8.0, the Single Sign-on (SSO) enhancement has been added to the HTML5 VNC Bookmark. You can choose to use either SSL VPN account credentials or custom credentials as the SSO credentials as shown below:



Edit Bookmark

Bookmark Name: * VNC

Name or IP Address: * 10.103.227.15:5901

Description:

Tabs:

Service: Virtual Network Computing (VNC – HTML5)

VNC Options

☐ View Only

☑ Share Desktop

☑ Automatically log in

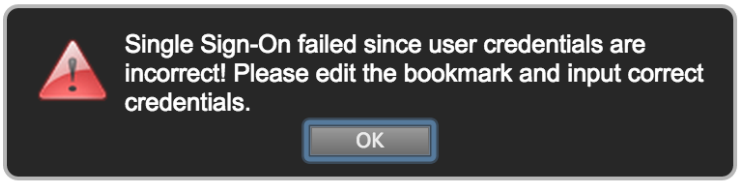
● Use SSL VPN account credentials

○ Use custom credentials

☐ Display Bookmark to Mobile Connect clients

If the SSO credential is correct, after you click the VNC - HTML5 Bookmark, you are logged in without having to enter a password.

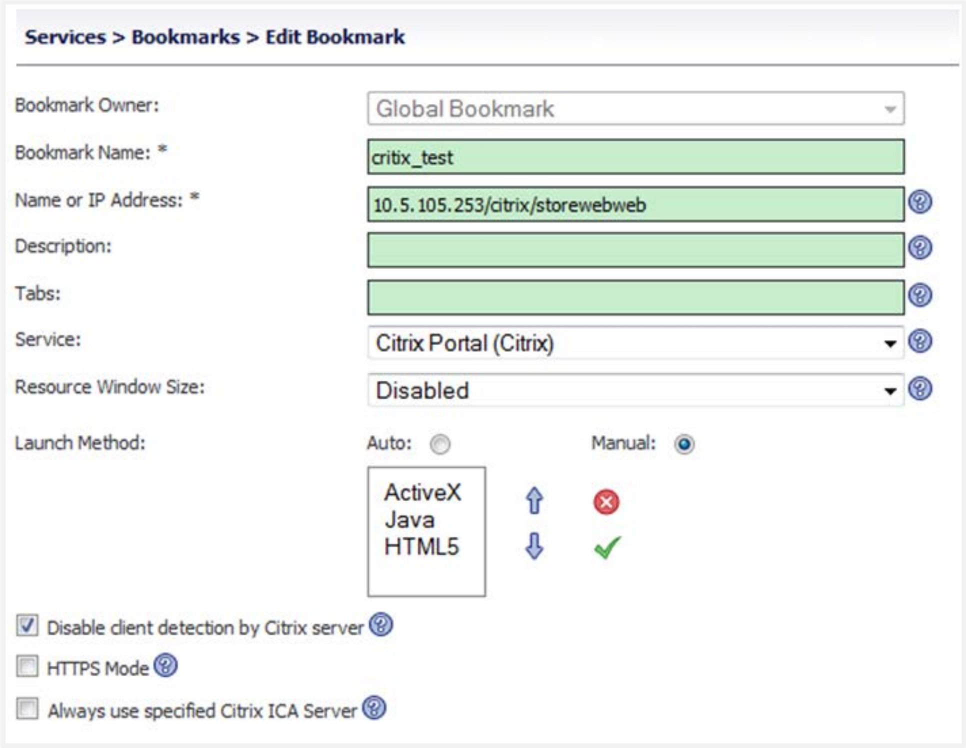
When the SSO credential is incorrect, you are asked to enter correct credentials by editing the bookmark.



Single Sign-On failed since user credentials are incorrect! Please edit the bookmark and input correct credentials.

Citrix HTML bookmark enhancement

This enhancement (Services > Bookmarks > Add/Update) consists of a new option **Launch Method** added when you configure Citrix bookmarks as shown below:



Services > Bookmarks > Edit Bookmark

Bookmark Owner:	Global Bookmark
Bookmark Name: *	critix_test
Name or IP Address: *	10.5.105.253/citrix/storewebweb
Description:	
Tabs:	
Service:	Citrix Portal (Citrix)
Resource Window Size:	Disabled
Launch Method:	Auto: ○ Manual: ●
	ActiveX Java HTML5

☑ Disable client detection by Citrix server

□ HTTPS Mode

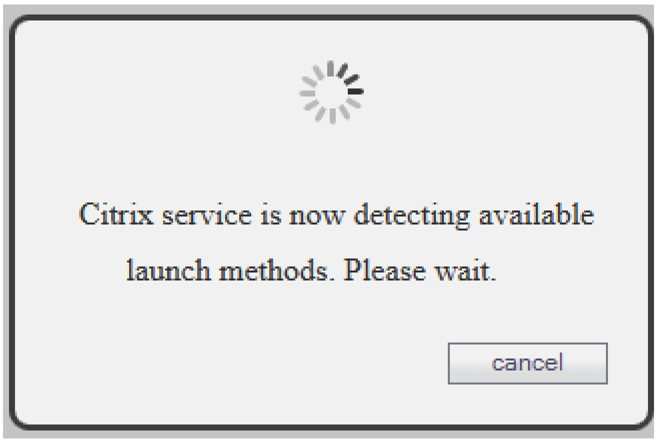
□ Always use specified Citrix ICA Server

The **Launch Method** option defaults to **Auto** when you create a new Citrix bookmark.

In **Manual**, you can change, enable or disable the method by clicking the icons to the right to select **ActiveX**, **Java**, or **HTML5**. In the mode you can also prioritize launch methods to be used using the Up and Down arrow buttons.

NOTE: The old option Always use Java in Internet Explorer is no longer available since you can choose which way to run Citrix after launching the bookmark as long as your browser and OS support it.

When you click a Citrix bookmark, a new message displays:



Citrix service is now detecting available launch methods. Please wait.

When the target Citrix server boots, it checks to see if HTML5 is supported. After the detection, you can choose one of the available methods or wait for the defaulted one to access Citrix service, or click Cancel to abort the launch process.

If there is no launch method available on your device, a warning message appears. Click OK to close the window and return to the Edit Bookmark page to reconfigure the method.

HTML5 File Sharing (CIFS/FTP)

In previous releases, SRA appliances had two types bookmark services:

- Common Internet File Share (CIFS)
- File Transfer Protocol (FTP).

Though they are different protocols, they are both used to share files.

SRA 8.0 provides a single user interface for the two services to operate with the remote sharing server. This new interface is scalable when expanding the browser, more convenient, and easier to use.

The file share feature has the normal actions: add, delete, rename, upload, download, login and logout.

Folders and Files Viewer

When you launch one FTP or CIFS type bookmark, it displays the file share interface with two panels. The left panel lists the folders in a tree viewer. You can click one folder icon or folder name to view its subdirectory. The right panel shows folders and files with a table viewer. You can double click one folder item to view its subdirectory. You can also drag the pointed axis to adjust the width between the two panels.

Address input

For CIFS clients:

1. Edit the address text area and input any target server you want to view.
2. If the server needs authentication, a pop-up a dialogue allows you to input user credentials.
3. When authentication is successful, the inputted user credentials are recorded and you can login later in the same session. If you logout from the CIFS client or the SRA appliance, all the user credentials are removed.

For FTP clients:

The address input is read-only and only shows the path you are viewing. Refer to the *SRA 8.0 Administration Guide* for more information.

Additional functionality

This new interface also provides the following functions:

- Add, Delete, Rename files and folders
- Drag files to upload them
- Download files
- Ftp Sessions
- Logout

Refer to the *SRA 8.0 Administration Guide* for more information about these functions.

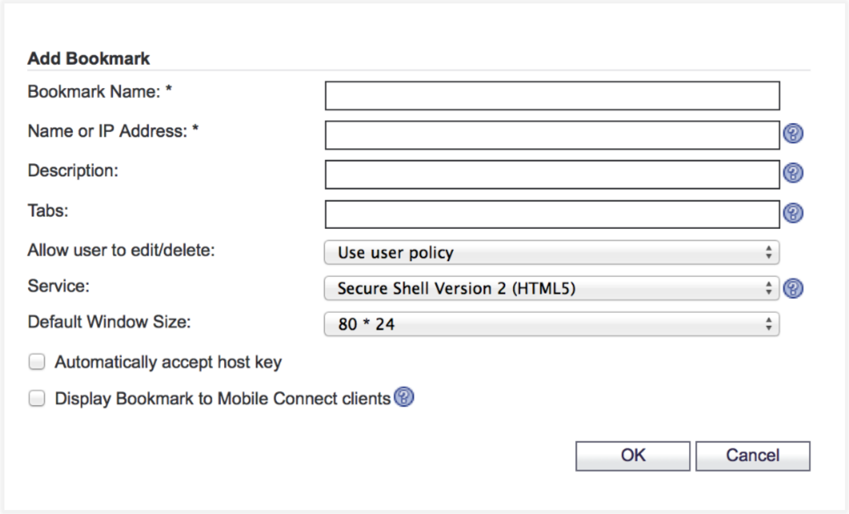
SSHv2 and Telnet HTML5 enhancements

SRA 8.0 provides new HTML5 enhancements for the following:

- SSHv2
- Telnet

SSHv2 HTML5 enhancement

SRA 8.0 provides SSHv2 access with HTML5 requests and replaces the applet version on browsers that support this functionality. The screen below shows the (Services > Bookmarks > Add/Update) setting page for the bookmark.



Add Bookmark

Bookmark Name: *

Name or IP Address: *

Description:

Tabs:

Allow user to edit/delete: Use user policy

Service: Secure Shell Version 2 (HTML5)

Default Window Size: 80 * 24

□ Automatically accept host key

□ Display Bookmark to Mobile Connect clients

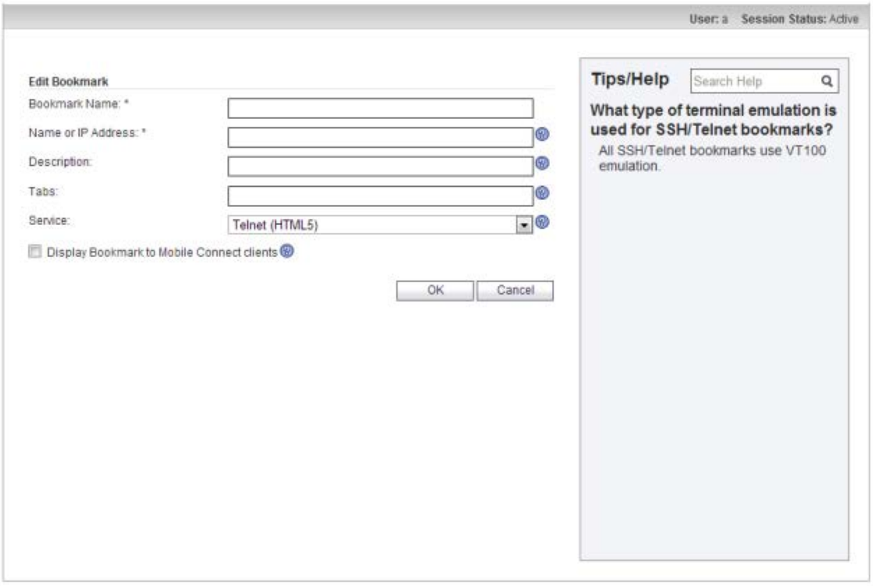
For the Default Window Size parameter, select the option with the maximum number of rows that can be displayed on the screen.

When you select the **Automatically accept host key** checkbox, the browsers keeps the server’s public host key in local storage automatically, otherwise it shows a confirmation message.

HTML5 Telnet Enhancement

SRA 8.0 provides telnet access with HTML5 requests that replace the older applet version on browsers that support this functionality. The bookmark, called “Telnet (HTML5),” starts a telnet HTML 5 client and needs no Java applet.

The following screen (Services > Bookmarks > Add/Update) shows the setting page for the bookmark.



User: a Session Status: Active

Edit Bookmark

Bookmark Name: *

Name or IP Address: *

Description:

Tabs:

Service: Telnet (HTML5)

□ Display Bookmark to Mobile Connect clients

What type of terminal emulation is used for SSH/Telnet bookmarks?

All SSH/Telnet bookmarks use VT100 emulation.

The telnet HTML5 client is a virtual terminal based on the telnet protocol. Most functions of VT100 are supported, including:

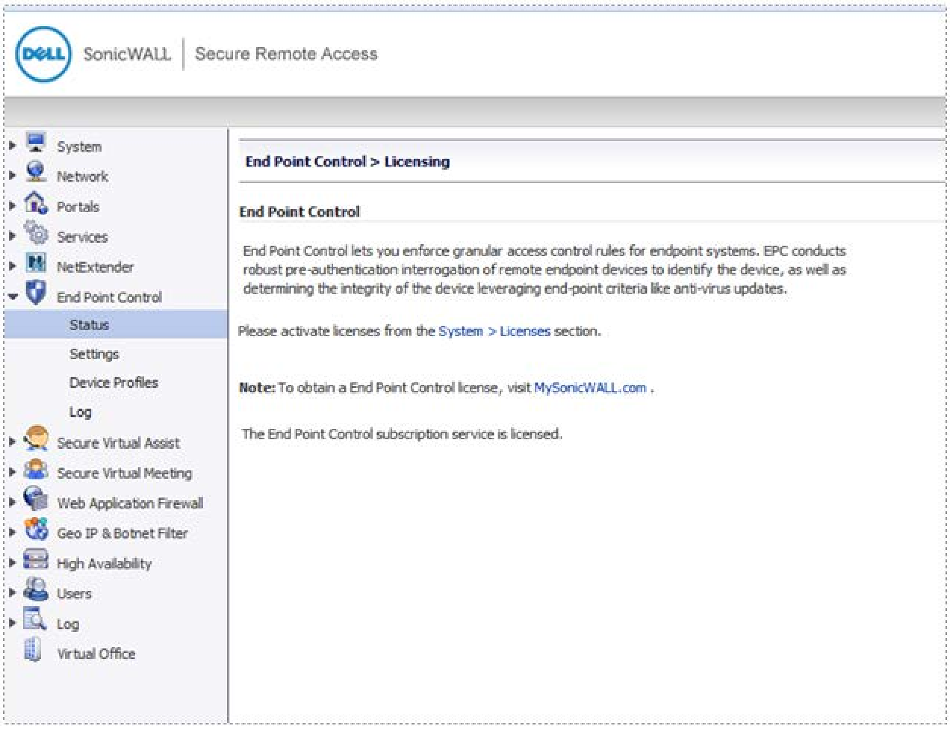
- Text input
- Coloring
- Position change
- Save/restore screen

EPC enhancements

The End Point Control (EPC) feature in the SRA 8.0 uses a third-party component from OPSWAT Inc. to evaluate the anti-virus, anti-spyware and personal firewall installed on a client's environment. The products from OPSWAT are updated frequently when their certificated vendors update them. Until SRA 8.0, the OPSWAT components were tightly bound to the firmware. But the firmware updates are not released as frequently as the OPSWAT components. In order to apply the latest OPSWAT updates, SRA updates the firmware with the OPSWAT updates. Otherwise, VPN clients including NetExtender or Mobile Connect may be unable to detect the latest published version of this protection software.

EPC is a license-free feature, but for OPSWAT the decoupled update is a licensed feature, so a license page is added to the EPC module to show the status of the OPSWAT. NetExtender clients for different platforms will detect the updates and automatically download and apply the new OPSWAT libraries.

If automatic updating from OPSWAT is not licensed, the license page appears similar to the following screen.



End Point Control > Licensing

End Point Control

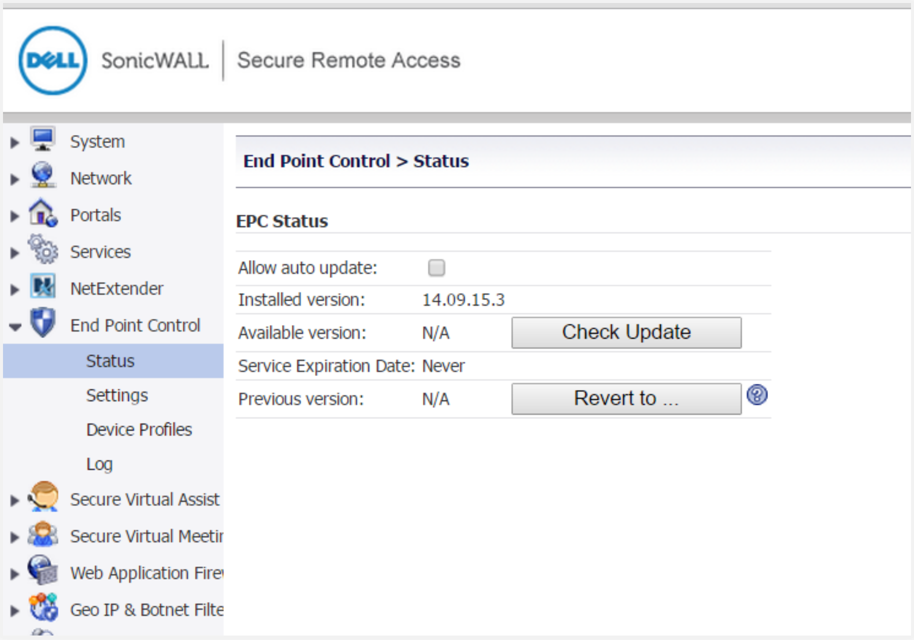
End Point Control lets you enforce granular access control rules for endpoint systems. EPC conducts robust pre-authentication interrogation of remote endpoint devices to identify the device, as well as determining the integrity of the device leveraging end-point criteria like anti-virus updates.

Please activate licenses from the System > Licenses section.

Note: To obtain a End Point Control license, visit MySonicWALL.com .

The End Point Control subscription service is licensed.

The EPC Status page appears as follows:



End Point Control > Status

EPC Status

Allow auto update: □
Installed version: 14.09.15.3
Available version: N/A
Service Expiration Date: Never
Previous version: N/A

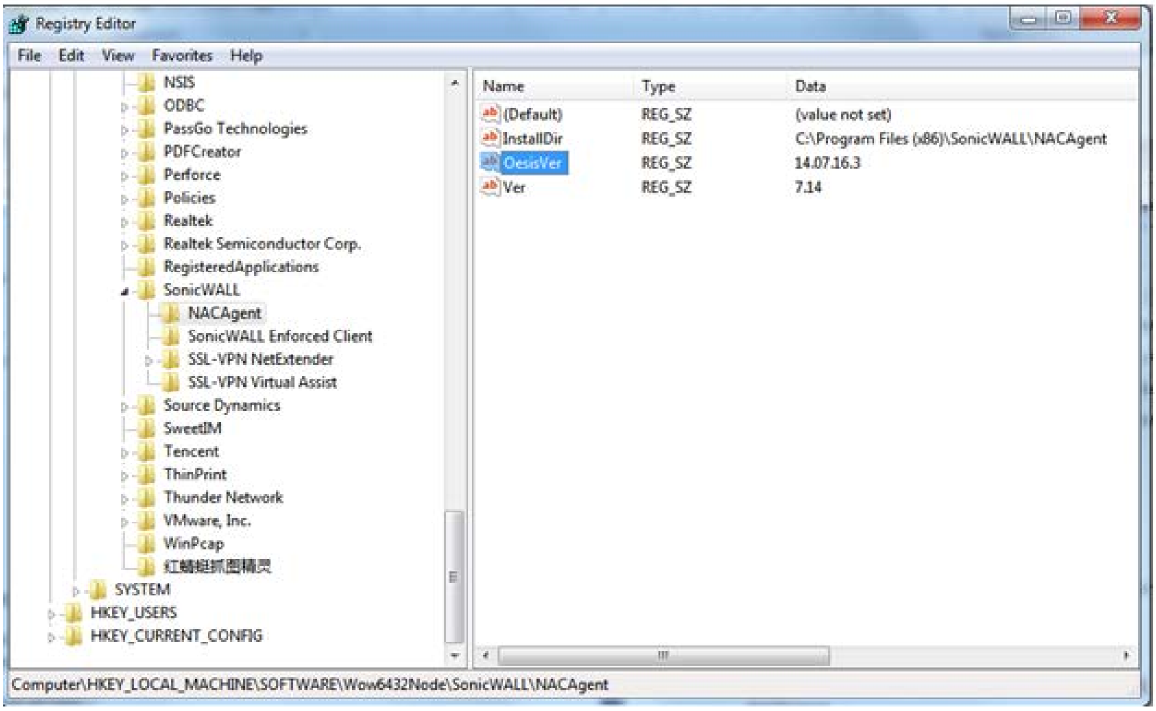
The status information is as follows:

- **Allow auto update** - This check box disables/enables the auto application of the OPSWAT update.
- **Check Update** - Typically, the SRA appliance checks updates periodically (every hour). When you click this button, update checking starts immediately.
- **Revert to** - Click this button to apply a previous good version.

Updates for Windows NetExtender

The latest NetExtender can check if the server has OPSWAT updates, automatically download the changes, and apply them before connection.

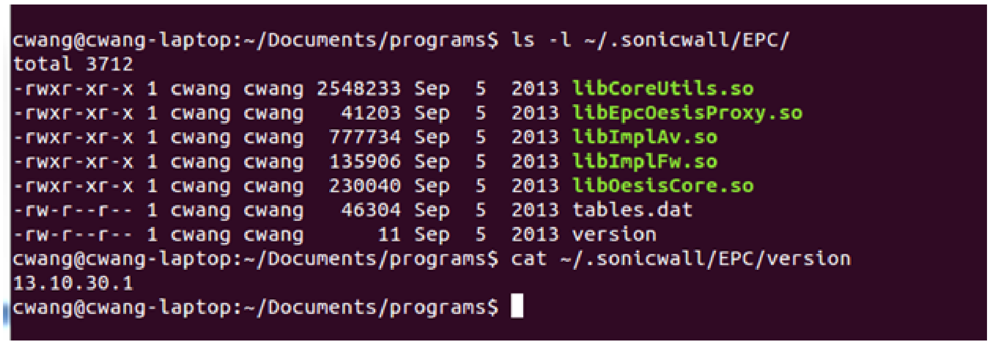
You can locate the currently installed OPSWAT version using the Registry Editor (NetExtender Windows client) shown below.



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallDir	REG_SZ	C:\Program Files (x86)\SonicWALL\NACAgent
OesisVer	REG_SZ	14.07.16.3
Ver	REG_SZ	7.14

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SonicWALL\NACAgent

For the Linux and Linux/Mac client, use the following path to find the version:



```
cwang@cwang-laptop:~/Documents/programs$ ls -l ~/.sonicwall/EPC/
total 3712
-rwxr-xr-x 1 cwang cwang 2548233 Sep  5  2013 libCoreUtils.so
-rwxr-xr-x 1 cwang cwang   41203 Sep  5  2013 libEpcOesisProxy.so
-rwxr-xr-x 1 cwang cwang  777734 Sep  5  2013 libImplAv.so
-rwxr-xr-x 1 cwang cwang  135906 Sep  5  2013 libImplFw.so
-rwxr-xr-x 1 cwang cwang  230040 Sep  5  2013 libOesisCore.so
-rw-r--r-- 1 cwang cwang   46304 Sep  5  2013 tables.dat
-rw-r--r-- 1 cwang cwang      11 Sep  5  2013 version
cwang@cwang-laptop:~/Documents/programs$ cat ~/.sonicwall/EPC/version
13.10.30.1
cwang@cwang-laptop:~/Documents/programs$ █
```

Application Offloading and HTTP Bookmark enhancements

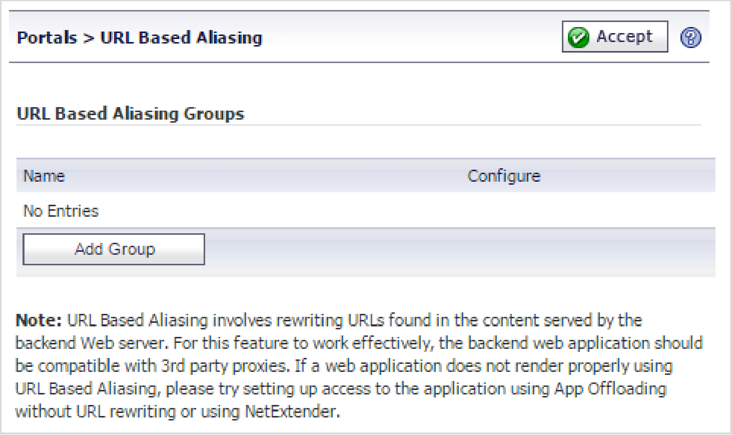
This SRA 8.0 enhancement includes the following features:

- **URL Based Aliasing** - Provides the ability to access several different web sites through one portal using one domain name.
- **Customized Favicon** - Provides the ability to specify a different Favicon for every portal. The Favicon of a backend server can be reused directly when authentication control is disabled.
- **Perfect Auto Scheme for Load Balancing Member** - Provides the ability to select a scheme automatically according to the scheme that you specified.

- **Advanced SSL/TLS Settings** - Provides the ability to set more detailed SSL/TLS settings per portal, including Enforce Forward Secrecy, Verify Backend SSL Server Certificate for Proxy connections and Force SSL/TLS version for Proxy connections.

URL Based Aliasing

The URL based Aliasing setting is designed to be consistent with the Load Balancing setting. The first step is to add a URL Based Aliasing group from Portals > URL Based Aliasing page as shown below.



Portals > URL Based Aliasing

URL Based Aliasing Groups

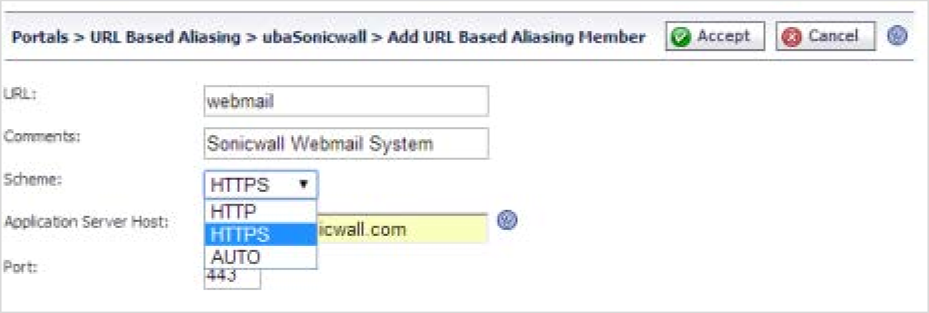
Name	Configure
No Entries	

Note: URL Based Aliasing involves rewriting URLs found in the content served by the backend Web server. For this feature to work effectively, the backend web application should be compatible with 3rd party proxies. If a web application does not render properly using URL Based Aliasing, please try setting up access to the application using App Offloading without URL rewriting or using NetExtender.

After adding a Group, you can click the Configure icon to add group memebers.

On the member settings page, configure the following settings:

- URL – This is used to access this specific member.
- Comments – Anything entered in this field displays on the Index page.
- Scheme – This defines the scheme of the backend server.
- Application Server Host – This field auto-populates based on your host.
- Port – The port value changes based on selected scheme.



Portals > URL Based Aliasing > ubaSonicwall > Add URL Based Aliasing Member

URL: webmail

Comments: Sonicwall Webmail System

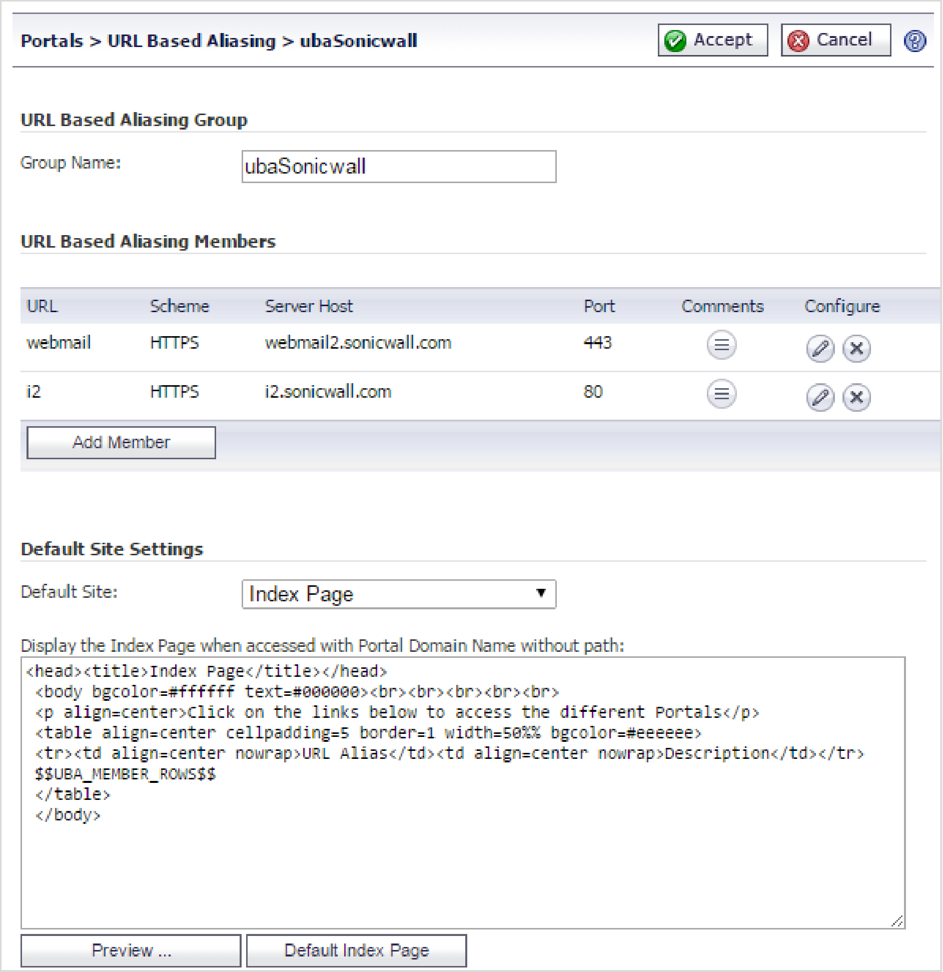
Scheme: HTTPS

Application Server Host: icwall.com

Port: 443

As many as 100 members can be added to one group. Members are listed on the Group Settings page. The “Default Site Settings” section provides the ability to set a default site when accessing the portal without any URL specified.

The default value is “Index Page” and can be previewed by clicking the **Preview** button. The Index page can be customized by editing the HTML and clicking **Accept**.



URL Based Aliasing Group

Group Name: ubaSonicwall

URL Based Aliasing Members

URL	Scheme	Server Host	Port	Comments	Configure
webmail	HTTPS	webmail2.sonicwall.com	443	☰	✎ ⊗
i2	HTTPS	i2.sonicwall.com	80	☰	✎ ⊗

Default Site Settings

Default Site: Index Page

Display the Index Page when accessed with Portal Domain Name without path:

```
<head><title>Index Page</title></head>
 <body bgcolor=#ffffff text=#000000><br><br><br><br><br>
 <p align=center>Click on the links below to access the different Portals</p>
 <table align=center cellpadding=5 border=1 width=50%% bgcolor=#eeeeee>
 <tr><td align=center nowrap>URL Alias</td><td align=center nowrap>Description</td></tr>
 $$UBA_MEMBER_ROWS$$
 </table>
 </body>
```

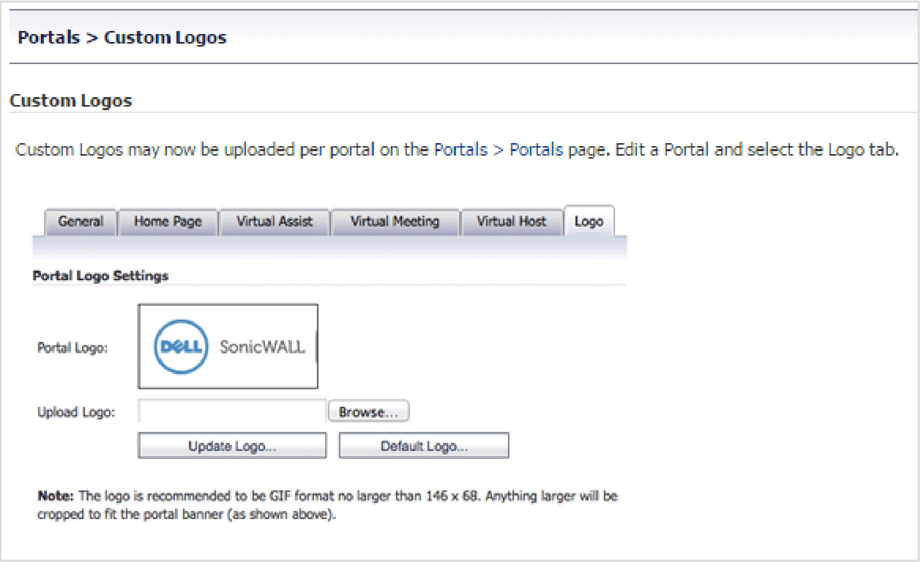
After a URL Based Aliasing group has been added, an Application Offloading Portal can then be created. From the Offloading tab, select the “Enable URL Based Aliasing” check box; the “Enable URL Rewriting for self-referenced URLs” option will automatically be selected. Select a URL Based Aliasing Group from the dropdown menu, then click **Accept** to save settings and create the portal.

Customized favicons

The Custom Logos setting page is under Portals > Custom Logos. A favorite logo is sometimes called a favicon. Customized Logo Settings is designed to be consistent with Portal Logo Settings.

- Click **Browse** to select a file and click Update Favicon… to upload it.
- Click **Default Favicon** to use the default favicon.

The **Reuse Favicon of Offloaded Server** checkbox is visible only when authentication control of the portal is disabled. When it is enabled, the Favicon of the backend server instead of the uploaded or the default one are displayed in the client browser.



Portals > Custom Logos

Custom Logos

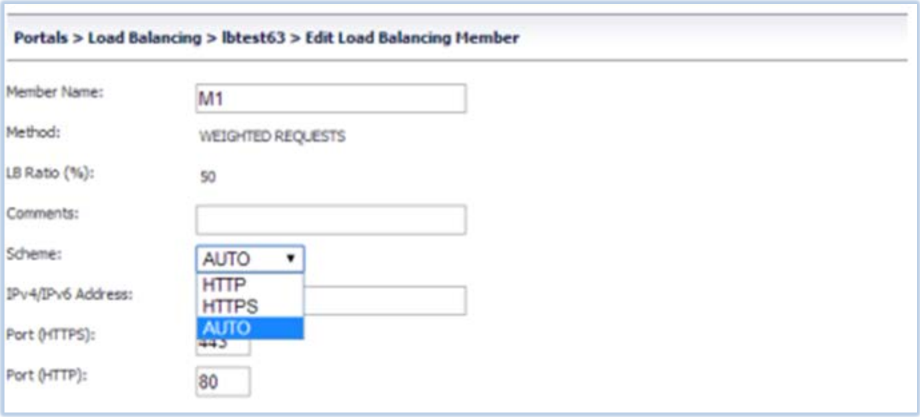
Custom Logos may now be uploaded per portal on the Portals > Portals page. Edit a Portal and select the Logo tab.

Note: The logo is recommended to be GIF format no larger than 146 x 68. Anything larger will be cropped to fit the portal banner (as shown above).

Auto scheme for Load Balancing member

Before SRA 8.0, the Scheme of Load Balancing Member could only be set to HTTP or HTTPS, which limits the functionality when the backend server can accept both HTTP and HTTPS connections. Now you can set the Scheme to AUTO. Load Balancing selects the proper scheme to connect to the backend server according to the scheme that you specify.

When you select Auto, you should also specify two port numbers (HTTPS and HTTP) as shown below.



Portals > Load Balancing > lbtest63 > Edit Load Balancing Member

Member Name: M1
Method: WEIGHTED REQUESTS
LB Ratio (%): 50
Comments:
Scheme: AUTO
IPv4/IPv6 Address:
Port (HTTPS): 443
Port (HTTP): 80

NOTE: To enable HTTP access for the App Offloading Portal, select the **Enable HTTP access** option under the Virtual Host tab of the Portal.

SharePoint 2013 App Offloading support

When the SharePoint 2013 server is accessed through an offloaded portal, its basic functions are supported, that is, adding/editing/deleting documents/tasks/calendar events.

Client integration is supported no matter whether the offloaded portal's authentication controls are enabled or disabled. But when the authentication controls are enabled, it's only supported on IE when:

- The offloaded portal created for the SharePoint 2013 uses a valid certificate.
- The scheme used by the offloaded portal and the backend SharePoint 2013 are the same. That is, if the backend SharePoint 2013 is running on HTTP, the offloaded portal should enable HTTP access and be accessed with HTTP. Otherwise if the backend SharePoint 2013 is running on HTTPS, the

offloaded portal should also be accessed with HTTPS. The same scheme also means URL Rewriting for the offloaded portal doesn't have to be enabled.

- The option Share session with other local applications of the offloaded portal is enabled.
- The option Restrict Request Headers at page Services > Settings is disabled.
- On the client, if the OS is Windows Vista or Windows 7, the offloaded portal should be added in the Trusted sites of the client's IE browsers.
- During login, the option Share session with other local applications is enabled.

When the OWA 2013 is accessed through an HTTP(S) Bookmark, the following features of OWA 2013 are supported:

- Mail (compose and send, attachment, delete, new email notification)
- Calendar (create, edit, delete, notification)
- Contact (create, edit, delete)
- Task (create, edit, delete)
- Logout

Virtual Assist/ Virtual Access/ Virtual Meeting enhancements

This feature concerns the Secure Virtual Assist application on the MacOS enhancements as follows:

- Unattended Mode
- Virtual Access Mode
- Wake on LAN (WOL)
- Session Record
- Digital certificate authentication without Username and Password

When active, these features may cause other features to run slower due to the traffic going through the appliance.

ⓘ **NOTE:** Backwards compatibility is not supported. All systems should be updated to the latest major version.

Unattended mode

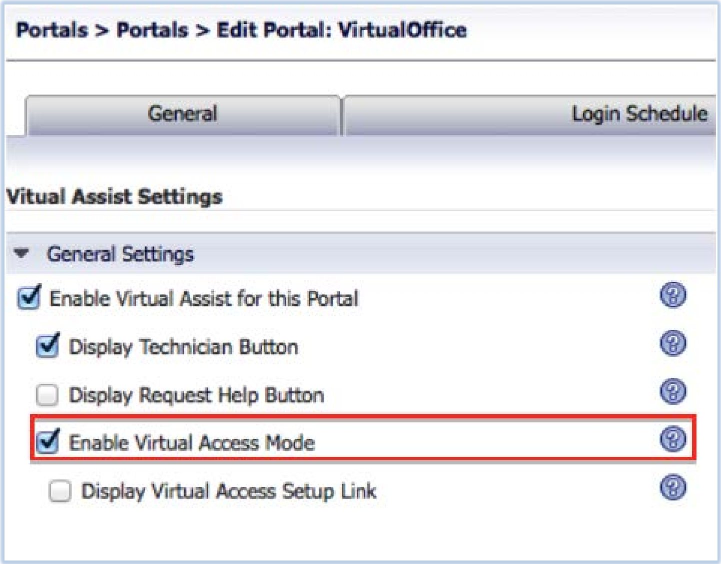
With proper permission, unattended mode allows the technician unrestricted access to the customer computer. This includes access to the system when the customer is not present. A password restricts access to the system from other technicians.

ⓘ **NOTE:** During the Unattended Mode, the system must keep active.

If the current mode is not Unattended Mode, use the **Change Mode** button to switch the mode. After switching, you can set the Unattended Mode parameters. Set the server address and access password, then login to the server.

Virtual Access mode

The Virtual Access feature is a tool to allow customers the ability to access their personal computers located outside the LAN of the SRA appliance. After selecting this mode and entering your credentials, you must also enable the **Virtual Access Mode** in Portal Settings at the web page as shown below.



Portals > Portals > Edit Portal: VirtualOffice

Vitual Assist Settings

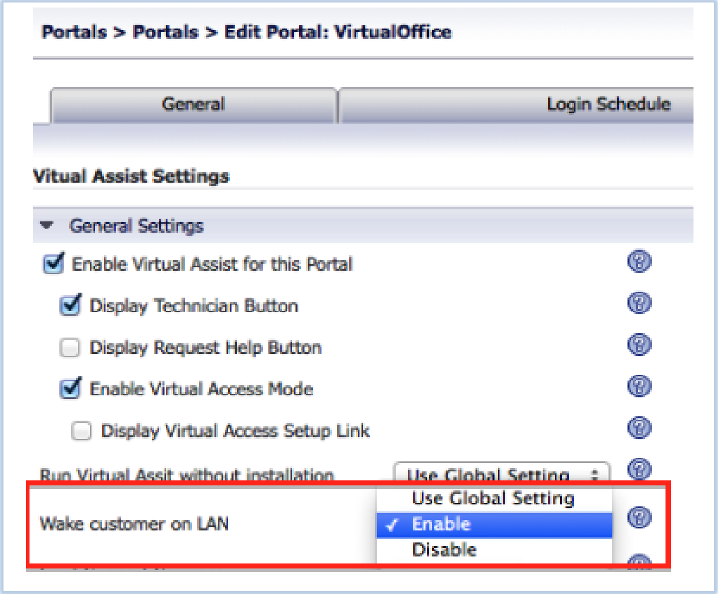
General Settings

- ☑ Enable Virtual Assist for this Portal
- ☑ Display Technician Button
- □ Display Request Help Button
- ☑ Enable Virtual Access Mode
- □ Display Virtual Access Setup Link

Wake on LAN (WOL)

This feature allows you to access a sleeping system. Activate this feature as follows:

1. Enable WOL on the portal (server).



Portals > Portals > Edit Portal: VirtualOffice

Vitual Assist Settings

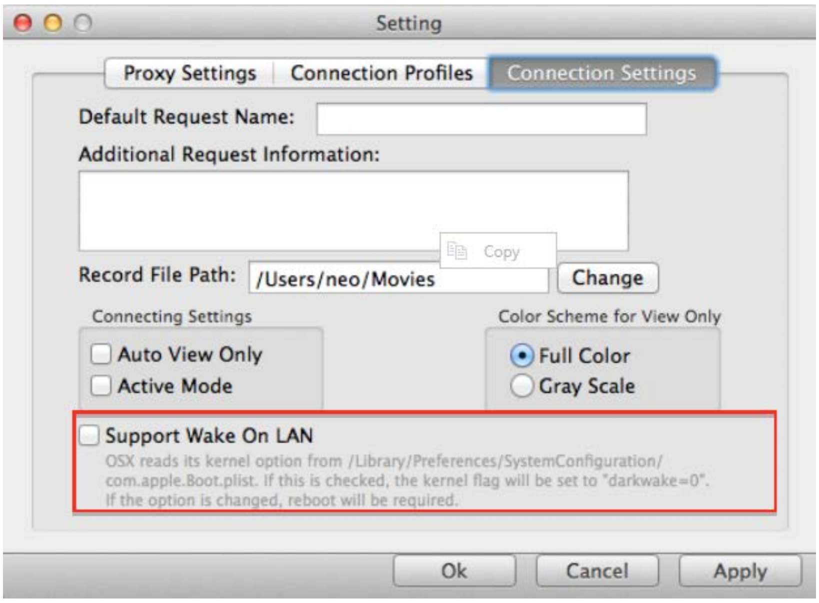
General Settings

- ☑ Enable Virtual Assist for this Portal
- ☑ Display Technician Button
- □ Display Request Help Button
- ☑ Enable Virtual Access Mode
- □ Display Virtual Access Setup Link

Run Virtual Assit without installation: Use Global Setting

Wake customer on LAN: Use Global Setting / ✓ Enable / Disable

2. Change the settings of the Virtual Assist Client by clicking **Support Wake on LAN**.



Default Request Name:

Additional Request Information:

Record File Path: /Users/neo/Movies

Connecting Settings

□ Auto View Only

□ Active Mode

Color Scheme for View Only

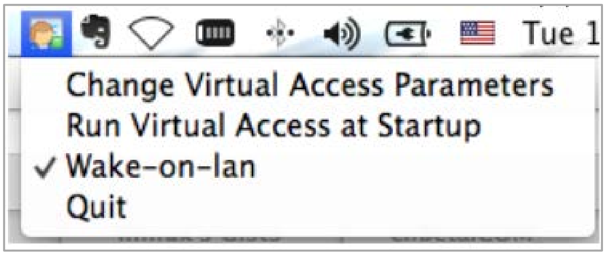
● Full Color

○ Gray Scale

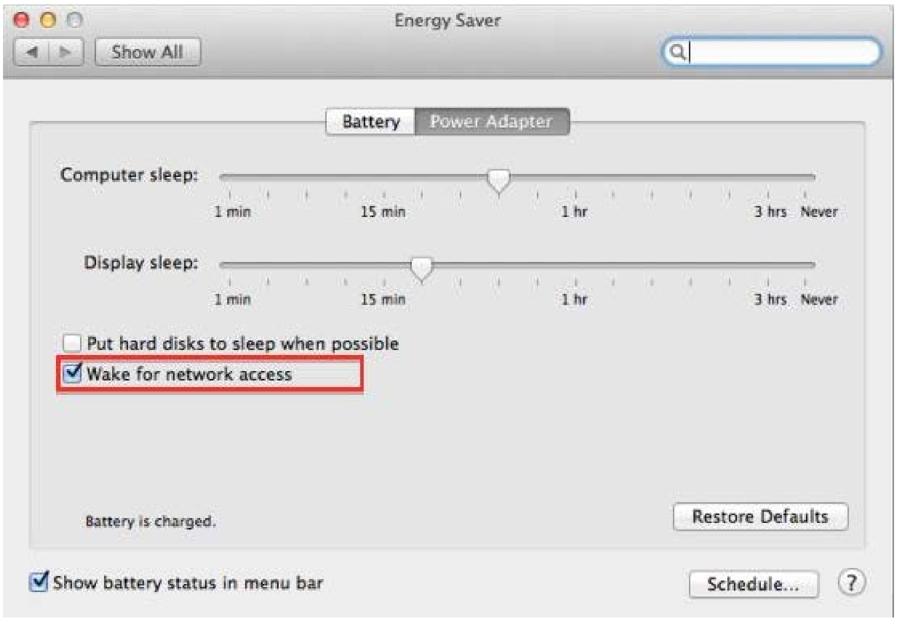
□ Support Wake On LAN

OSX reads its kernel option from /Library/Preferences/SystemConfiguration/com.apple.Boot.plist. If this is checked, the kernel flag will be set to "darkwake=0". If the option is changed, reboot will be required.

3. Click **OK**.
4. Enable **Wake-on-lan** on the Status Popup Menu.


Tue 1
Change Virtual Access Parameters
Run Virtual Access at Startup
✓ Wake-on-lan
Quit

5. On the System Preferences page, click **Energy Saver**.
6. On the System Preferences > Energy Saver page, select **Wake for network access**.



Computer sleep:

Display sleep:

□ Put hard disks to sleep when possible

☑ Wake for network access

Battery is charged.

☑ Show battery status in menu bar

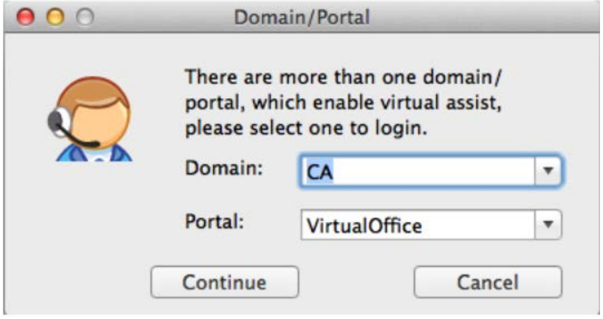
Session record

The Session Record feature works in Technician Mode only and allows you to record the support process. You can configure the video file path from the Virtual Assist Preferences screen.

Digital Certificate Authentication

Digital certificate authentication is a new authentication mode that allows you to log in to the SRA Server without a Username or Password. In the SRA 8.0, the Virtual Assist Client supports it, but it only works in Technician Mode. Use the following steps:

1. Select the Digital Certificate Authentication Domain.



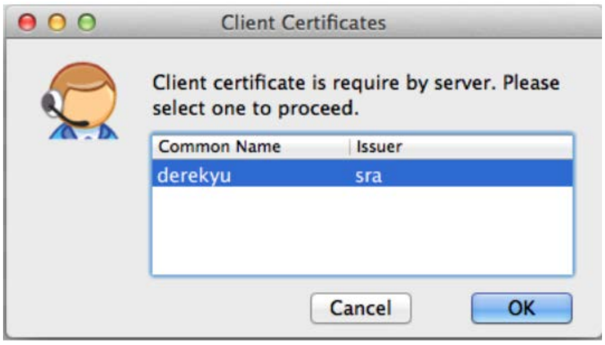
Domain/Portal

There are more than one domain/portal, which enable virtual assist, please select one to login.

Domain: CA

Portal: VirtualOffice

2. Use the client pop up window to select the right client certificate. Then, log in to the server.



Client Certificates

Client certificate is require by server. Please select one to proceed.

Common Name	Issuer
derekyu	sra

Secure Virtual Meetings on MacOS

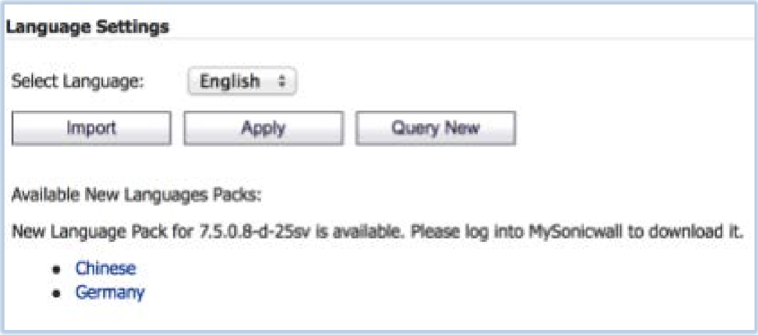
SRA 8.0 supports Secure Virtual Meetings on the MacOS client. The owner of the meeting must be a user with Virtual Meeting privileges on the appliance. The coordinator does the meeting setup and is in control of the meeting. Scheduling and meeting settings are done by the coordinator, who owns the meeting. For more information and configuration procedures, refer to the *SRA 8.0 Administration Guide*.

Localization enhancements

Since there have been more customer requests for international languages, SRA 8.0 includes enhancements for the user to import language packs to firmware. In this way, multiple languages can be supported dynamically, and have language packs independent of the firmware.

Language Packs

SRA 8.0 has added a new section, Language Settings, to the System > Settings page.



Language Settings

Select Language: English

Available New Languages Packs:

New Language Pack for 7.5.0.8-d-25sv is available. Please log into MySonicwall to download it.

- Chinese
- Germany

After a new language pack is imported, it appears in the Language Settings list.

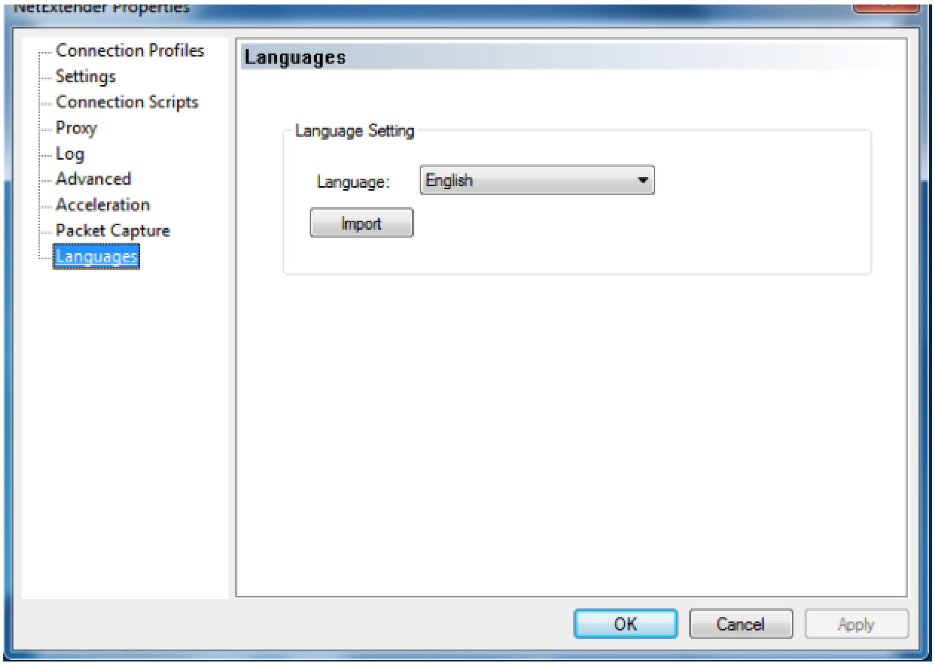
The language packs are stored on a backend server. The firmware checks the backend server every hour, and you can manually query the available language packs on the backend server by clicking the **Query New** button. If there are any new language packs available, they are listed. You can download the packs by clicking the link.

Stand-alone clients

NetExtender

The newly designed localization enhancement separates the user interface-specific resources from the NetExtender client. Then the language package can be dynamically imported into to the NetExtender client. To support a new language, it only needs to be translated for the specific resources and imported in that language into NetExtender, with no need to release new firmware to support the language.

You can import a language package through the NetExtender settings page.



NetExtender Properties

Languages

Language Setting

Language: English

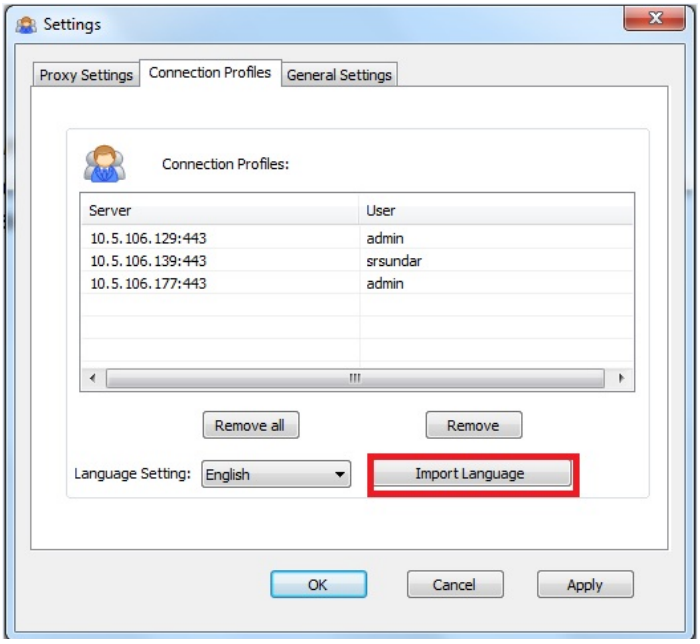
After the language is imported, it appears in the drop down list.

You can switch languages by selecting the language from the drop-down list or from the menu context. You must restart the NetExtender GUI to make the language take effect.

After you change the language setting, you should also localize NetExtender Log Viewer, NEGLI and NetExtender logon dialer.

Secure Virtual Meeting Windows client

You can import a new language package to Secure Virtual Meeting. All language packages are ZIP format files. Click the **Import Language** button to select the package.



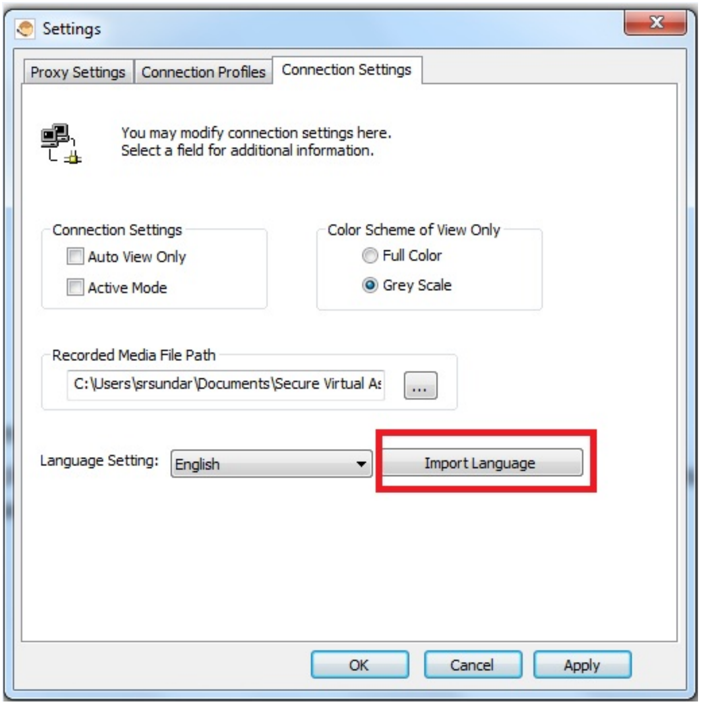
Connection Profiles:

Server	User
10.5.106.129:443	admin
10.5.106.139:443	srsundar
10.5.106.177:443	admin

Language Setting: English

Secure Virtual Assist Windows client

You can also import new language packages to Secure Virtual Assist. All language packages are ZIP Format files. Click the **Import Language** button to select the package.



You may modify connection settings here.
Select a field for additional information.

Connection Settings
□ Auto View Only
□ Active Mode

Color Scheme of View Only
○ Full Color
● Grey Scale

Recorded Media File Path
C:\Users\srsundar\Documents\Secure Virtual As

Language Setting: English

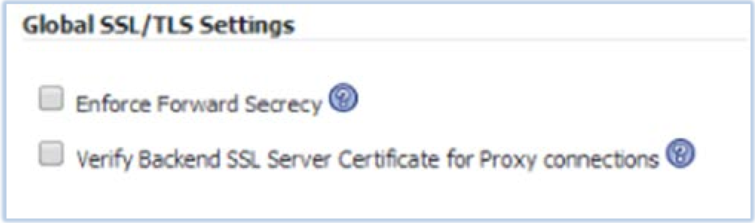
Miscellaneous enhancements

SRA 8.0 provides the following various enhancements:

- Perfect Forward Secrecy
- CA Authentication and Authorization
- Email/Auto-Email Settings on Upgrade
- Scheduled Settings
- Hide Domains During Login
- User Name and Domain Binding
- Configuration and Portal Settings

Perfect forward secrecy

You can set Advanced SSL/TLS settings globally on the System > Administration page, including **Enforce Forward Secrecy** and **Verify Backend SSL Server Certificate for Proxy connections**.

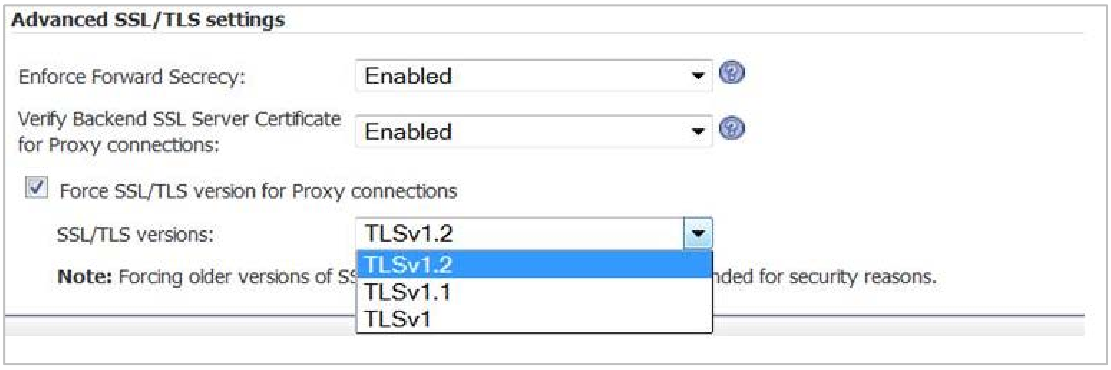


Global SSL/TLS Settings

□ Enforce Forward Secrecy

□ Verify Backend SSL Server Certificate for Proxy connections

You can also set the following options per portal under the Virtual Host tab.



Advanced SSL/TLS settings

Enforce Forward Secrecy:	Enabled
Verify Backend SSL Server Certificate for Proxy connections:	Enabled

☑ Force SSL/TLS version for Proxy connections

SSL/TLS versions: TLSv1.2

Note: Forcing older versions of S nded for security reasons.

NOTE: Forward Secrecy allows current information to be kept secret even if the private key is compromised in the future. Browsers that do not support Forward Secrecy may not be able to connect to the SRA. Performance may also decline depending on the ciphers that the client browser supports.

When you enable **Verify Backend SSL Server Certificate for Proxy connections**, connections to the backend server may be dropped when the backend server certificate is not trusted. The verification depth is 10. Alert level log messages are also generated.

The **Force SSL/TLS version for Proxy connections** option is used to support old style backend servers that only support specific version of SSL/TLS. This option is not recommended for security reasons.

CA authentication and authorization

Previously, Dell SonicWALL SSL-VPN appliances had to verify usernames and passwords before client certificate authentication. SRA 8.0 provides client certificate-based authentication without username and password. This feature uses a certificate attribute, such as OU or ++ CN, as the login username to the appliance and for later authorization.

NOTE: Authentication without username/password is now supported on Secure Virtual Meeting and Secure Virtual Assist, and NetExtender clients using Digital Certificate authentication.

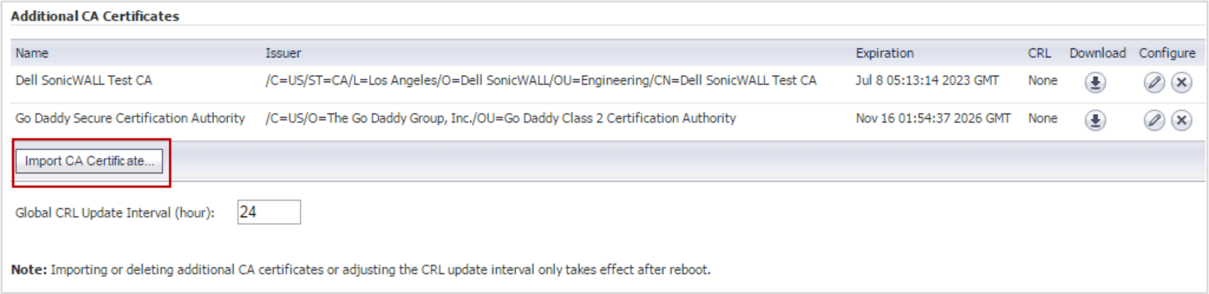
This section includes information about the following:

- Viewing the CA Certificate
- Adding a Digital Certificate Type Domain
- Authentication
- Authorization

NOTE: When upgrading to SRA 8.0, make sure all previous CA certificates are correctly in the All CA certificates list. If they are not, remove the previous one and import it again.

Viewing the CA certificate list

Before importing a CA certificate, view the CA list as shown below on the System > Certificates settings page. The Import CA Certificate is highlighted.



Additional CA Certificates

Name	Issuer	Expiration	CRL	Download	Configure
Dell SonicWALL Test CA	/C=US/ST=CA/L=Los Angeles/O=Dell SonicWALL/OU=Engineering/CN=Dell SonicWALL Test CA	Jul 8 05:13:14 2023 GMT	None	⬇	✎ ✕
Go Daddy Secure Certification Authority	/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority	Nov 16 01:54:37 2026 GMT	None	⬇	✎ ✕

Global CRL Update Interval (hour): 24

Note: Importing or deleting additional CA certificates or adjusting the CRL update interval only takes effect after reboot.

Adding a Digital Certificate type domain

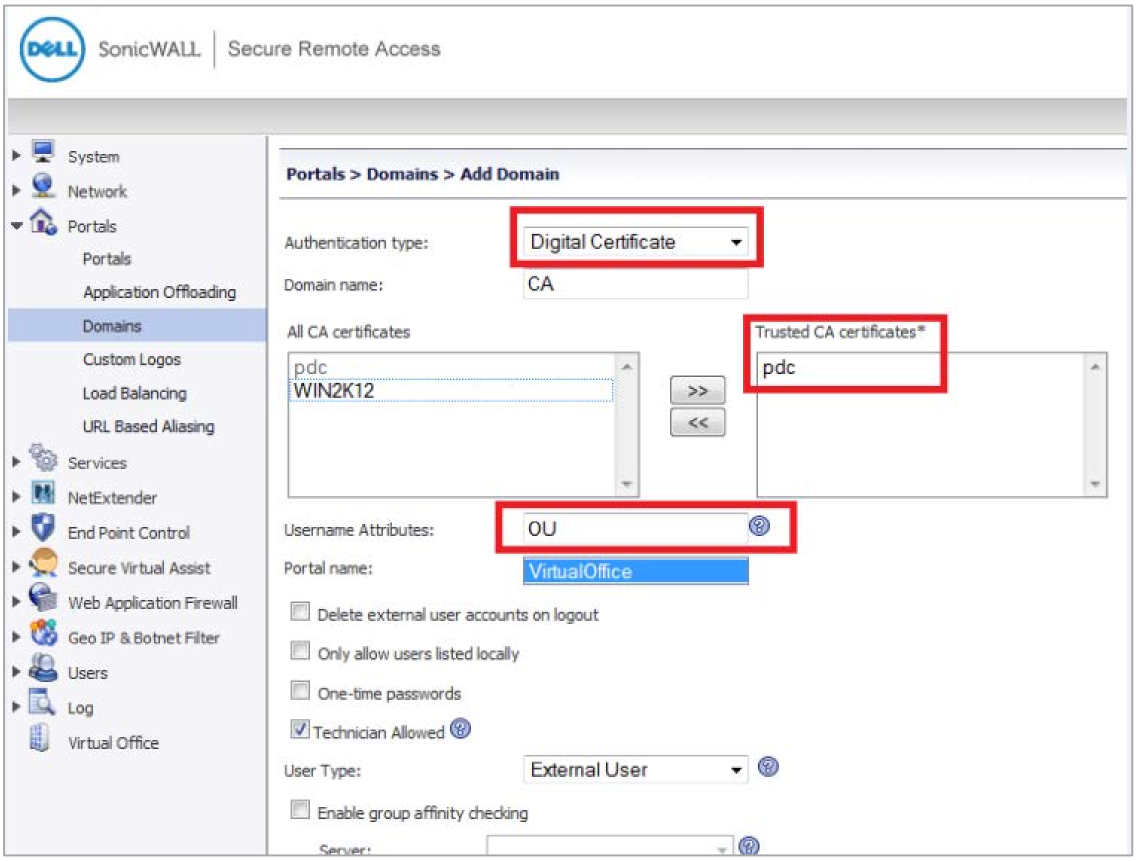
Add a Digital Certificate Type Domain as explained and illustrated below. If no User Attribute is provided or the attribute provided is not present in the certificate by default, the certificate name is used as username.

1. Click the **Import CA Certificate** button.
2. Add a new domain, and select the authentication type **Digital Certificate**.
3. Choose one or more certificates from the **All CA certificates** list and move it (them) to the **Trusted CA certificates** list.

   The **All CA certificates** list contains all available certificates of the appliance which have been imported from the system certificate setting.

   The **Trusted CA certificates** list contains all available certificates for this domain.

4. Set **OU** as the Username Attribute, which means the system will use the value of the OU attribute of the client certificate as the login username.



Portals > Domains > Add Domain

Authentication type: Digital Certificate

Domain name: CA

All CA certificates: pdc, WIN2K12

Trusted CA certificates*: pdc

Username Attributes: OU

Portal name: VirtualOffice

□ Delete external user accounts on logout

□ Only allow users listed locally

□ One-time passwords

☑ Technician Allowed

User Type: External User

□ Enable group affinity checking

Server:

Authentication

Before logging in, import the client certificate to your browser. From the Certificates settings window of your browser, select the CA domain and select a client certificate to authenticate from the pop-up dialogue box. If the CA of the client certificate is a member of the Trusted CA certificates list, the authentication is complete.

If the issuer of the client certificate is not in the Trusted CA certificates list, the system blocks the access and generates an on-screen error message.

Authorization

Before authorizing a client certificate user, the system must know the group of the user. This is done by enabling group affinity checking and selecting one domain as the server to get group information for the user. As the target group server, the system only supports the Active Directory type server and the LDAP type server. The selectable target server is the appliance available Active Directory / LDAP domain.

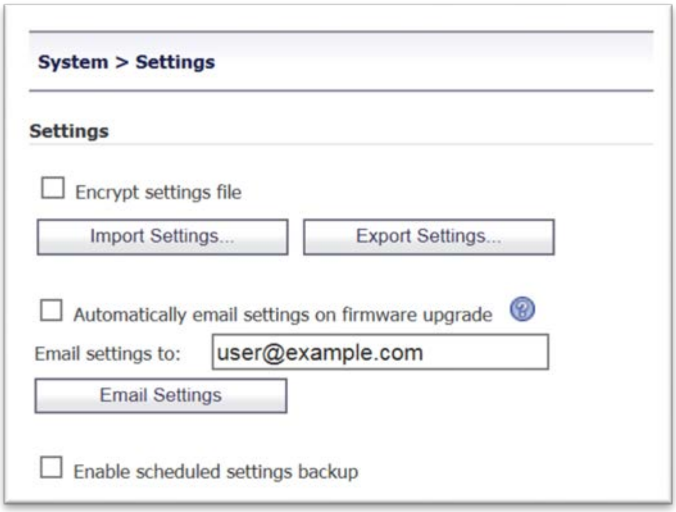
Once the system has the external group information, you can choose one group as the primary group for the user, and set different group policies for the different groups. Using the group policy, you can authorize the login user to different resources.

Email/Auto-Email settings on upgrade

This release adds options to email settings for administrative users. It is also possible to automatically email the settings on a firmware upgrade.

This allows users to revert back to their working environment if they are not happy after an upgrade. It is easy for TAC to assist them to get back up and running with a working configuration.

Administrators can also request the current configuration to be emailed to a specified email address. When you do this, make sure to specify a valid Mail Server and Mail from Address in the Log > Settings page for the settings to be emailed as shown below.



□ Encrypt settings file

□ Automatically email settings on firmware upgrade

Email settings to: user@example.com

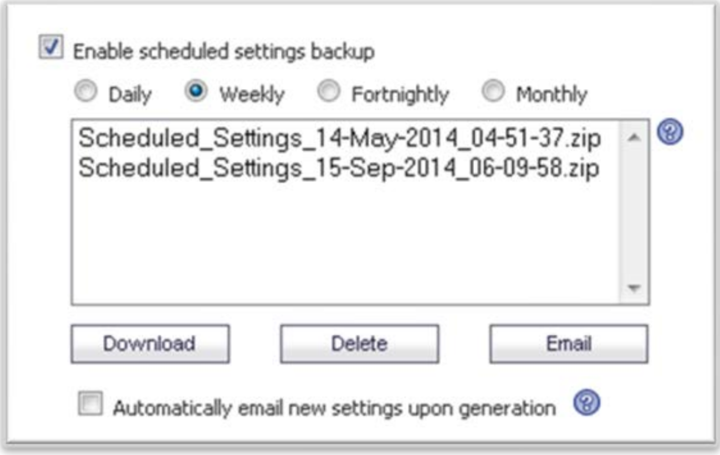
□ Enable scheduled settings backup

Scheduled settings

You can now specify a periodic backup of your appliance settings for Daily, Weekly, Fortnightly or Monthly. The generated settings are stored in the appliance configuration file and listed for easy manageability. Up to a maximum of 6 settings can be stored in the configuration file or a combined disk size of 10 MB after which it is rotated.

Similar provision exists to automatically email the settings upon generation, provided the required mail settings are configured in the appliance from Log > Settings page.

The naming convention for the generated file is Scheduled_Settings_dd-mon-yyyy_hh-mm-ss.zip as illustrated below.



☑ Enable scheduled settings backup

○ Daily ● Weekly ○ Fortnightly ○ Monthly

Scheduled_Settings_14-May-2014_04-51-37.zip
Scheduled_Settings_15-Sep-2014_06-09-58.zip

□ Automatically email new settings upon generation

NOTE: SRA services (Easy Access) must be restarted when you toggle between the options or disable the Scheduled Settings altogether.

Username and domain binding

On the Users > Local Users page, an administrator can add a user with the same name for different domains and apply a different policy for each one.

Configuration and portal settings

Configuration is specified on two levels: portal and user as shown below. The user level configuration takes a higher priority than the portal level.

In the User Settings, when you select **Enforce login uniqueness** as **Use Portal Setting**, the configuration in portal takes effect.

If you enable **Enforce login uniqueness**, the following occurs:

- When the **Enforcement** method is selected to **Automatically logout existing session**, the existing session is stopped automatically by the coming login event.
- When the **Enforcement method** is selected to **Confirm logout of existing session**, a confirmation dialog pops up to choose whether to stop the existing session. If yes, the existing session is stopped and the login process continues. If not, the login process is aborted.

For Configuration in Domain Settings, configuration is specified in two levels, domain and user. The user level configuration takes higher priority than portal level.

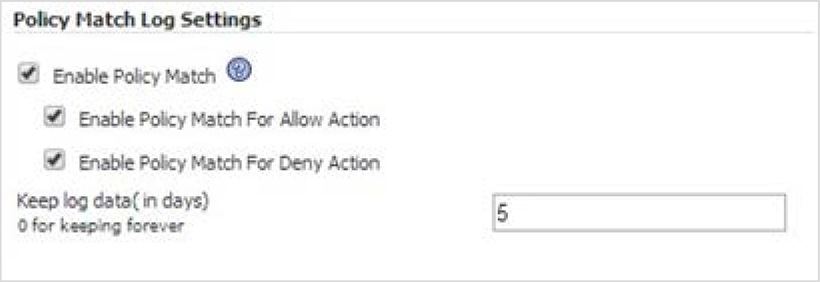
In Configuration in User Settings, when you select **Technician Allowed** as **Use Domain Setting**, the configuration in domain takes effect. When **Technician Allowed** is enabled, Virtual Assist can log in as a technician. If disabled, the user belonging to that domain may only raise requests.

When you access one or more services, you can match policies defined by the SRA appliance's administrator. SRA 8.0 provides more statistical information for policies, for example, how many times each policy was used, who matches the policy, where the user comes from, and so on.

The Administrator can now allow/prevent downloading of the Secure Virtual Assist client from the support Login page by configuring it the same in Virtual Assist Settings in the portal.

Policy match logging

You can configure various policies on the SRA appliance to control the access to a LAN. In previous releases, a limited amount of data was logged when policy items were matched.



Policy Match Log Settings

☑ Enable Policy Match

☑ Enable Policy Match For Allow Action

☑ Enable Policy Match For Deny Action

Keep log data(in days)
0 for keeping forever: 5

You can view the statistic information for policies on Services > Policies page by administrators shown below.

You can view the detailed policy matched log by clicking the images in the Statistic column. This feature is enabled/disabled by the administrator. The administrator can set the server log matched information to allow type, deny type and both. And the administrator can also set the life cycle of the logged data. If the logged data has expired, it is removed.

There are two data viewers: Statistic viewer and Detailed viewer. In the Statistic viewer, each policy has a column of various statistics. You can view the total matched count for the policy or click the image to view the detailed matched log of the policy.

Resolved issues

The following is a list of resolved issues in this release.

Authentication

Resolved issue	Issue ID
Certificate-based authentication needs user authentication, and asks to download the certificate. Occurs when importing CA certificates and then rebooting the SRA appliance. Upon creating a new Domain and enabling client certificate enforcement, the system will still ask to download the certificate again.	137211

Bookmarks

Resolved issue	Issue ID
The HTML5 RDP bookmark disconnects when launching Microsoft Word, and a “Connection Closed” notification displays. Upon reconnecting to the HTML5 RDP bookmark, Microsoft Word is open. Occurs when opening Microsoft Word when connected to an HTML5 RDP bookmark. Other Microsoft office applications have no effect on the HTML5 RDP bookmark connection.	154603
ActiveX Citrix bookmarks do not work with an untrusted SSL certificate. Occurs when using a Citrix bookmark with Internet Explorer 11 without Java enabled. The ICA client does not load.	152972
The HTML5 RDP bookmark does not work on Chrome version 37.0.2062.124. Occurs when using HTML5 RDP bookmarks on a Microsoft Windows 7. The bookmark does not open when using a Chrome browser. **Workaround:** Use a Firefox browser.	152410

Endpoint Control

Resolved issue	Issue ID
The Endpoint Control plug-in does not install when using a Firefox browser. Occurs when EPC is enabled and using Firefox version 19.	154610

GeoIP/Botnet

Resolved issue	Issue ID
GeoIP and Botnet policies cannot be exported or imported. Occurs when exporting and importing settings for GeoIP and Botnet policies.	151222
Logs generate for the GeoIP/Botnet service when GeoIP/Botnet settings are not enabled. The database is locked for GeoIP/Botnet and some of the SRA user interface pages are not visible. Occurs when the GeoIP/Botnet service is licensed, but not enabled. **Workaround:** Rebooting the SRA appliance resolves the issue for approximately 3-5 hours.	129488

High Availability

Resolved issue	Issue ID
A High Availability pair between two SRA Virtual Appliances in an Active or Idle state changes to a bad state after a failover. Occurs when changes are made to the LAN Monitoring address, causing a failover. The primary appliance does not failover to the secondary appliance because there is no HA link established. **Workaround:** Shut down one of the peers and disable the “Primary Appliance” check box on the active unit. Then, power on the peer unit.	154533

Using more than three CA certificates does not sync between appliances configured for High Availability. Occurs when using High Availability with two SRA Virtual Appliances. Once High Availability is synched, CA certificates that are uploaded do not sync.	154312

NetExtender

Resolved issue	Issue ID
The Post Connection Script File has an upload limitation. Occurs when uploading a script file over 2KB.	153701
NetExtender disconnects when using Microsoft Windows 10 Tech Preview. Occurs when using Microsoft Windows 10 Tech Preview and launching NetExtender.	153458

System

Resolved issue	Issue ID
SRA does not send syslogs to the GMS appliance, which results in GMS determining that the SRA appliance is down. No reports are logged on the GMS appliance. Occurs when the primary SRA appliance has a failover to the secondary SRA appliance. **Workaround**: Add both the primary and secondary appliances on GMS to receive reports.	150073
User is able to access the X1 interface using the IP address configured for the X0 interface. Occurs when connecting directly to the X1 interface and configuring the NIC gateway to the X1 IP address. **Workaround:** Deploy the SRA appliance in one-arm mode.	143779

Web Application Firewall

Resolved issue	Issue ID
Web Application Firewall (WAF) blocks access to websites when the CSRF mode is configured to "Detect Only" and a "Session Expired" notification displays. When the CSRF mode is configured to "Disabled," then access to websites is available. Occurs when attempting to access a website whilst WAF is enabled and the CSRF mode is configured to "Detect Only." The "Detect Only" setting should log the event and not restrict access.	146208

Known issues

The following is a list of known issues in this release.

Bookmarks

Known issue	Issue ID
Citrix bookmarks do not work with Internet Explorer 9. Occurs when using Internet Explorer 9 to launch a Citrix bookmark.	157952
HTML5 RDP bookmark does not work with Internet Explorer. Occurs when NLA is enabled.	157169
HTML5 RDP bookmark does not work with a Danish/German keyboard. Occurs when using Apple iOS or Android tablets to access HTML5 RDP bookmarks.	156273

Endpoint Control

Known issue	Issue ID
OPSWAT does not upgrade when the appliance is upgraded to SRA 8.0. Occurs when using a portal and Endpoint Control is enabled and upgraded from SRA 7.5 to SRA 8.0.	158070
OPSWAT does not upgrade when the appliance is upgraded to SRA 8.0. Occurs when NetExtender and Endpoint Control are enabled and upgraded from SRA 7.5 to SRA 8.0.	158068
The Endpoint Control > Status page displays 'N/A' instead of displaying the base version of EPC. Occurs when viewing the Endpoint Control > Status page after updating to SRA 8.0. The installed version only displays after using 'Apply Update.'	153704

Virtual Assist

Known issue	Issue ID
Occurs when the logging in as a Technician on a Virtual Appliance. The user is able to log in to the proxy, but after closing the session and logging in again, the proxy credentials are not saved and the user is prompted to re-enter credentials.	157818

NetExtender

Known issue	Issue ID
NetExtender does not properly work with IPv6. Occurs when using an IPv6 DHCP server. If IPv6 addresses are configured for X0/X1 interfaces and IPv6 DHCP Server is selected, NetExtender clients cannot acquire the IPv6 addresses.	157818
NetExtender Routes information displays when Tunnel All mode is enabled. Occurs when Tunnel All mode is enabled on NetExtender. A message should display that NetExtender is connected in Tunnel All mode and should not display route information.	157595
Uninstalling NetExtender on Linux/Mac machines does not completely remove certificate or log files. Occurs when uninstalling NetExtender on a Linux machine (netExtenderClient > /uninstallNetExtender) or on a Mac machine (Applications > uninstall NetExtender).	155881

Virtual Assist

Known issue	Issue ID
Proxy credentials do not save after a Technician logs in. Occurs when the logging in as a Technician on a Virtual Appliance. The user is able to log in to the proxy, but after closing the session and logging in again, the proxy credentials are not saved and the user is prompted to re-enter credentials.	157589

System compatibility

This section provides additional information about hardware and software compatibility with this release.

SRA appliance information

Although all SRA appliances support major SRA features, not all features are supported on all SRA appliances. The following section describes similarities and differences between appliances and supported features.

Similarities

The Dell SonicWALL SRA appliances and SRA Virtual Appliance share most major SRA features, including:

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

Differences

Important differences between the SRA appliances are shown in the table below. An 'X' indicates that the feature is supported on that appliance model.

Feature	SRA 4600	SRA 4200	SRA 1600	SRA 1200	SRA Virtual Appliance
Application Profiling	X	X			X
High Availability (HA)	X	X			X
Virtual Meeting	X	X			X

Product licensing

The Dell SonicWALL SRA 8.0 firmware provides user-based licensing on Dell SonicWALL SRA appliances and SRA Virtual Appliance. Licensing is controlled by the Dell SonicWALL license manager service, and customers 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 SRA 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 in to 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 or virtual appliance, perform the following steps:

1. Login 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 login to 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 login to update the license information on the appliance itself.
4. For the SRA 4600/4200/1600/1200 appliances, MySonicWALL automatically retrieves the serial number and authentication code. For the virtual appliance, you will need to enter this information:
   - Type the serial number of the virtual appliance into the Serial Number field. The serial number and authentication code are provided when the software is purchased.
   - Type the authentication code into the Authentication Code field.
5. Type a descriptive name for the appliance or virtual appliance into the Friendly Name field, and then click Submit.
6. Click Continue after the registration confirmation is displayed.
7. Optionally upgrade or activate licenses to other services displayed on the System > Licenses page.
8. After activation, view the System > Licenses page to see a cached version of the active licenses.

Upgrading information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the following sections:

Obtaining the latest SRA image version

To obtain a new SRA firmware image file for your Dell SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.

> **NOTE:** If you have already registered your Dell SonicWALL 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. Copy the new SRA image file to a directory on your management station.
   For the Dell SonicWALL SRA 4600/4200/1600/1200 appliance, this is a file such as:

   sw_sslvpnsra4600_eng_8.0.0.0_8.0.0_p_14sv_768935.sig

   For the Dell SonicWALL Virtual Appliance, this is a file such as:

   sw_sslvpnsra-vm_eng_8.0.0.0_8.0.0_p_14sv_768935.sig

> **NOTE:** For SRA Virtual Appliances, image files for new deployments have an .ova file extension, and image files for upgrades have a .sig file extension.

Exporting a copy of your configuration settings

Before beginning the update process, export a copy of your Dell SonicWALL SRA appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your Dell SonicWALL SRA appliance, 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.

ⓘ **Tip:** To more easily restore settings in the future, rename the .zip file to include the version of the Dell SonicWALL SRA image from which you are exporting the settings.

Uploading a new SRA image

Dell SonicWALL SRA appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a Dell SonicWALL SRA image, you must select **Uploaded Firmware with Factory Defaults**. You can then import a settings file saved from the previous version or reconfigure manually.

1. Download the SRA 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 SRA image file, select the file, and click the **Upload** button. The upload process can take up to one minute.
3. When the upload is complete, you are ready to reboot your Dell SonicWALL SRA appliance with the new SRA image. Do one of the following:

- To reboot the image with current preferences, click the boot icon for **Uploaded Firmware – New!**
- To reboot the image with factory default settings, click the boot icon for **Uploaded Firmware with Factory Defaults – New!**

ⓘ **Note:** Be sure to save a backup of your current configuration settings to your local computer before rebooting the Dell SonicWALL SRA appliance with factory default settings, as described in the previous “Saving a Backup Copy of Your Configuration Settings” section.

4. A warning message dialog is displayed saying *Are you sure you wish to boot this firmware?* Click **OK** to proceed. After clicking **O**K, do not power off the device while the image is being uploaded to the flash memory.
5. After successfully uploading the image to your Dell SonicWALL SRA appliance, the login screen is displayed. The updated image information is displayed on the System > Settings page.

Resetting the Dell SonicWALL SRA appliances using SafeMode

If you are unable to connect to the Dell SonicWALL security appliance’s management interface, you can restart the Dell SonicWALL security 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 Dell SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the Dell SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.

Note: The Dell SonicWALL security 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.

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

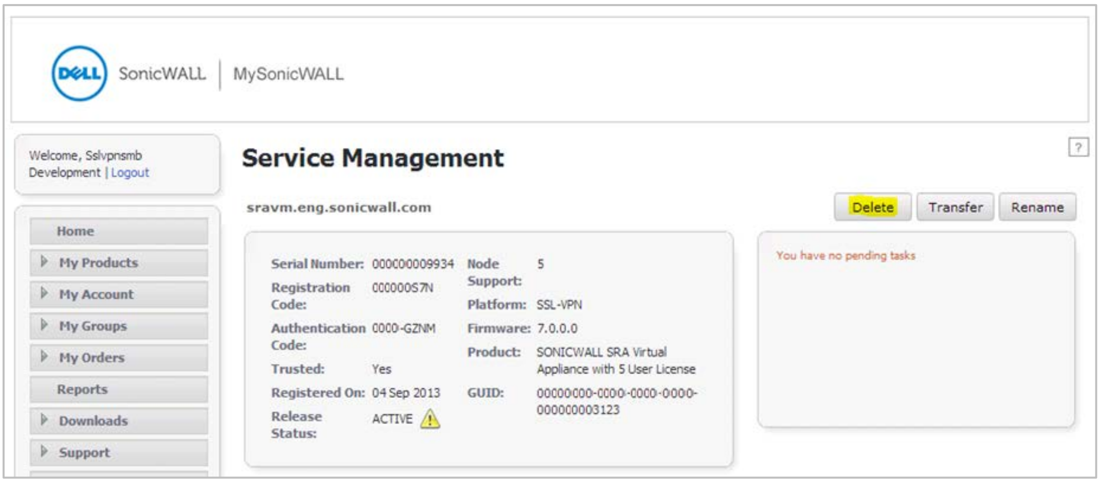
3. Connect to the management interface by pointing the Web browser on your management station to http://192.168.200.1. The SafeMode management interface displays.
4. Try rebooting the Dell SonicWALL security appliance with your current settings. Click the boot icon in the same line with Current Firmware.
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 SRA image with the factory default settings. Click the boot icon in the same line with Current Firmware with Factory Default Settings.

Moving a Virtual Appliance to SRA 8.0

A Virtual Appliance running SRA 7.5 can be upgraded to SRA 8.0 using a .sig file, from the System > Settings page.

A Virtual Appliance running SRA 7.0, or older, cannot be upgraded to SRA 8.0 because of operating system changes in the 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 on page 41.
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. Deploy a new virtual appliance using the SRA 8.0 OVA file available from www.mysonicwall.com.
5. Power on the new virtual appliance and configure the X0 interface using the CLI.
6. Log into the new virtual appliance as “admin” and import your saved configuration settings.
7. In MySonicWALL, click on the serial number of the old virtual appliance. On the Service Management page for it, click the Delete button to delete licensing for the old virtual appliance. If you are unable to delete the licensing, contact Dell SonicWALL support.



Service Management

sravm.eng.sonicwall.com

Serial Number: 000C00009934
Registration Code: 000000S7N
Authentication Code: 0000-GZNM
Trusted: Yes
Registered On: 04 Sep 2013
Release Status: ACTIVE ⚠
Node Support: 5
Platform: SSL-VPN
Firmware: 7.0.0.0
Product: SONICWALL SRA Virtual Appliance with 5 User License
GUID: 00000000-0000-0000-0000-000000003123

You have no pending tasks

8. Register the new virtual appliance from the System > Licenses page. Enter the serial number and authentication code.
This transfers all the licensed services from the old virtual appliance to the new virtual appliance.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to http://software.dell.com/support/.

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.

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

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

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

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

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

Patents

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

Trademarks

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

Legend

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

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

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

Last updated: 3/26/2015

232-002806-00 Rev A