# Release Notes

Secure Remote Access

**Dell SonicWALL SRA 7.5.0.0**

## Contents

## Platform Compatibility

The Dell SonicWALL SRA 7.5.0.0 release is supported on the following platforms:

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

## Licensing on the Dell SonicWALL SRA Appliances and Virtual Appliance

The Dell SonicWALL SRA 7.5.0.0 firmware provides user-based licensing on Dell SonicWALL SRA appliances and the SRA Virtual Appliance. Concurrent user sessions are limited to the number of user licenses.

| User Licenses | SRA 4600 | SRA 4200 | SRA 1600 | SRA 1200 | SRA Virtual Appliance |
|---|---|---|---|---|---|
| Included by default | 25 | 25 | 5 | 5 | 5 |
| Recommended number | 100 | 100 | 25 | 25 | N/A |
| Maximum number | 500 | 500 | 50 | 50 | 50 |

***Note**: The recommended number of users supported is based on factors such as access mechanisms, applications accessed and application traffic being sent. There is no recommended number for the SRA Virtual Appliance, as it depends on the underlying hardware.*

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. On the SRA 4600/4200, extra licenses are added in 10, 25, and 100 user denominations. On the SRA 1600/1200 and Virtual Appliance, customers can add licenses in 5-user and 10-user denominations.

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.

## Important Differences between the SRA Appliances

Although all SRA appliances support major SRA features, not all features are supported on all SRA appliances.

### *Similarities*

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

- End Point Control
- Geo IP & Botnet Filter
- NetExtender
- Virtual Access
- Virtual Assist
- Virtual Office
- Web Application Firewall

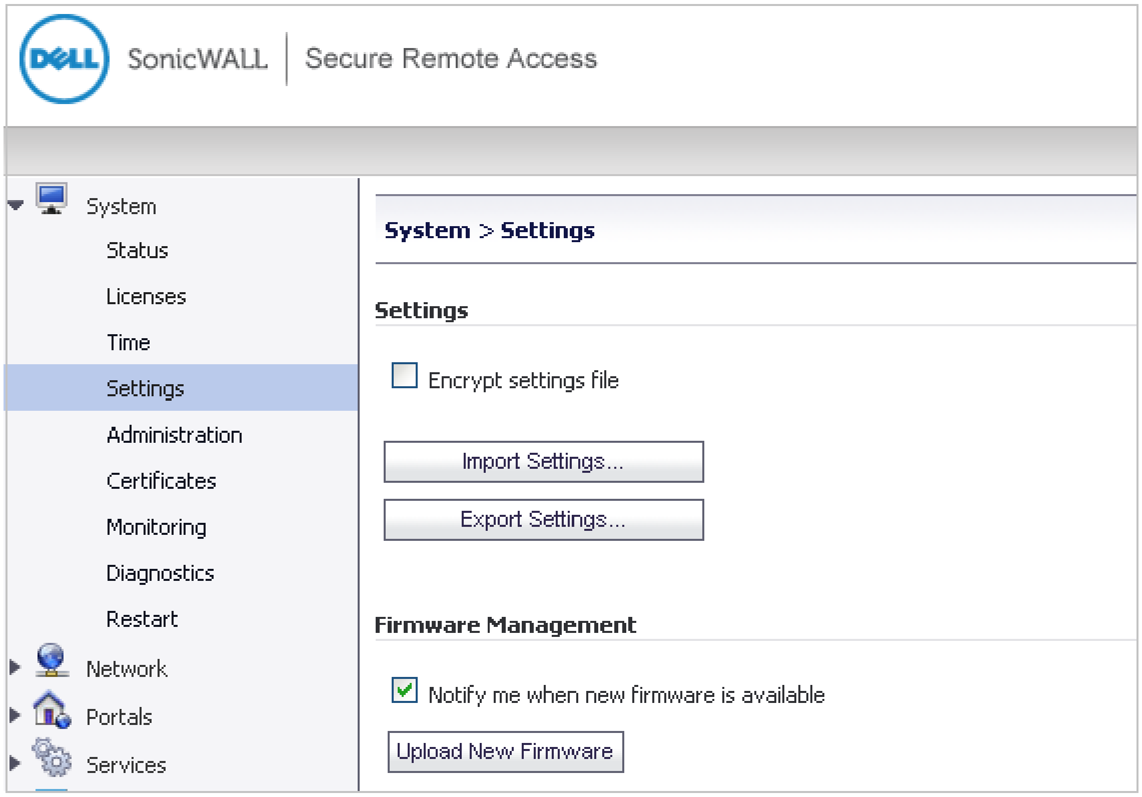
### *Differences*

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

| 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 |

The following are examples of the different System > Settings pages on the SRA Virtual Appliance and SRA hardware appliances:

- System > Settings page for the SRA Virtual Appliance:



System > Settings

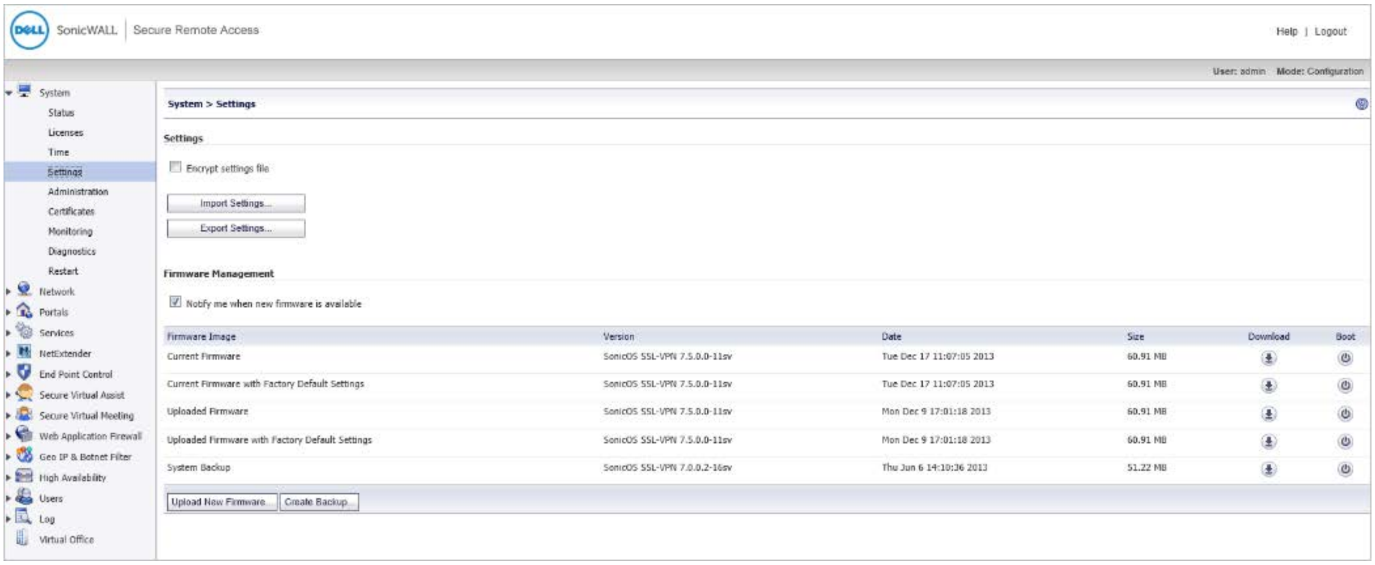
Settings

☐ Encrypt settings file

Firmware Management

☑ Notify me when new firmware is available

- System > Settings page for the SRA hardware appliances:



System > Settings

Settings

☐ Encrypt settings file

Firmware Management

☑ Notify me when new firmware is available

| Firmware Image | Version | Date | Size | Download | Boot |
|---|---|---|---|---|---|
| Current Firmware | SonicOS SSL-VPN 7.5.0.0-11sv | Tue Dec 17 11:07:05 2013 | 60.91 MB | ⭳ | ⏻ |
| Current Firmware with Factory Default Settings | SonicOS SSL-VPN 7.5.0.0-11sv | Tue Dec 17 11:07:05 2013 | 60.91 MB | ⭳ | ⏻ |
| Uploaded Firmware | SonicOS SSL-VPN 7.5.0.0-11sv | Mon Dec 9 17:01:18 2013 | 60.91 MB | ⭳ | ⏻ |
| Uploaded Firmware with Factory Default Settings | SonicOS SSL-VPN 7.5.0.0-11sv | Mon Dec 9 17:01:18 2013 | 60.91 MB | ⭳ | ⏻ |
| System Backup | SonicOS SSL-VPN 7.0.0.2-16sv | Thu Jun 6 14:10:36 2013 | 51.22 MB | ⭳ | ⏻ |

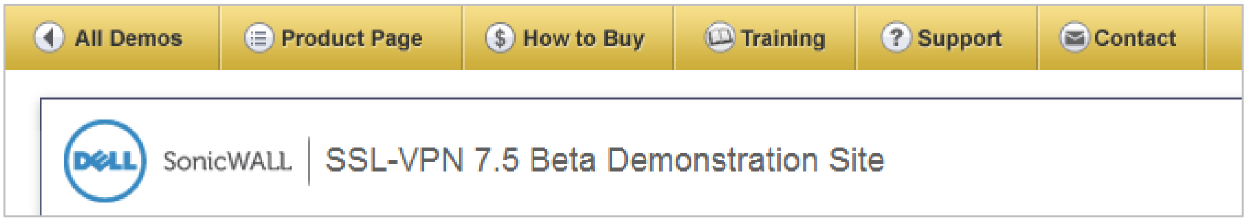
## Feature Enhancements in Dell SonicWALL SRA 7.5

The following enhancements and new features are introduced in the Dell SonicWALL SRA 7.5 release:

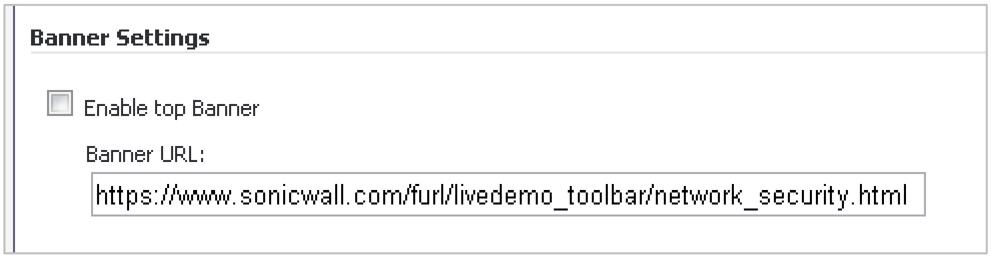
### *Customer Requested Enhancements and Minor Enhancements*

The following customer requested enhancements have been added to SRA 7.5:

- Demo Banner – A configurable link to another site can be displayed at the top of all SRA pages. By default the Dell SonicWALL live demo banner is displayed when a top banner is enabled:



Use the Banner Settings section of the <sslvpn>/cgi-bin/diag > Internal Settings page to configure the banner you want to display:

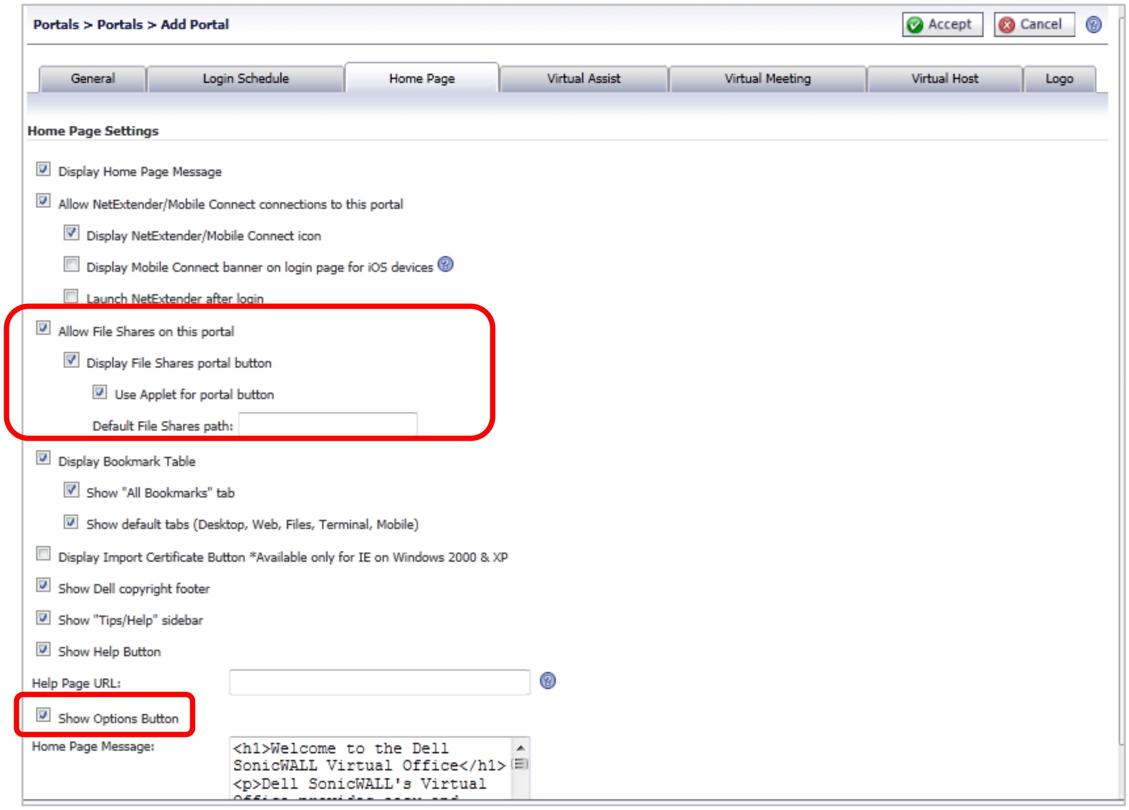


Banner Settings

□ Enable top Banner

Banner URL: https://www.sonicwall.com/furl/livedemo_toolbar/network_security.html

- Options button – The Options button shown at the top of the Secure Virtual Office page can now be hidden. Check the **Show Options Button** check box on the Home Page tab of the Portals > Portals > Add Portals page to display the Options button.



Home Page Settings

☑ Display Home Page Message

☑ Allow NetExtender/Mobile Connect connections to this portal

☑ Display NetExtender/Mobile Connect icon

☐ Display Mobile Connect banner on login page for iOS devices

☐ Launch NetExtender after login

☑ Allow File Shares on this portal

☑ Display File Shares portal button

☑ Use Applet for portal button

Default File Shares path:

☑ Display Bookmark Table

☑ Show "All Bookmarks" tab

☑ Show default tabs (Desktop, Web, Files, Terminal, Mobile)

☐ Display Import Certificate Button *Available only for IE on Windows 2000 & XP

☑ Show Dell copyright footer

☑ Show "Tips/Help" sidebar

☑ Show Help Button

Help Page URL:

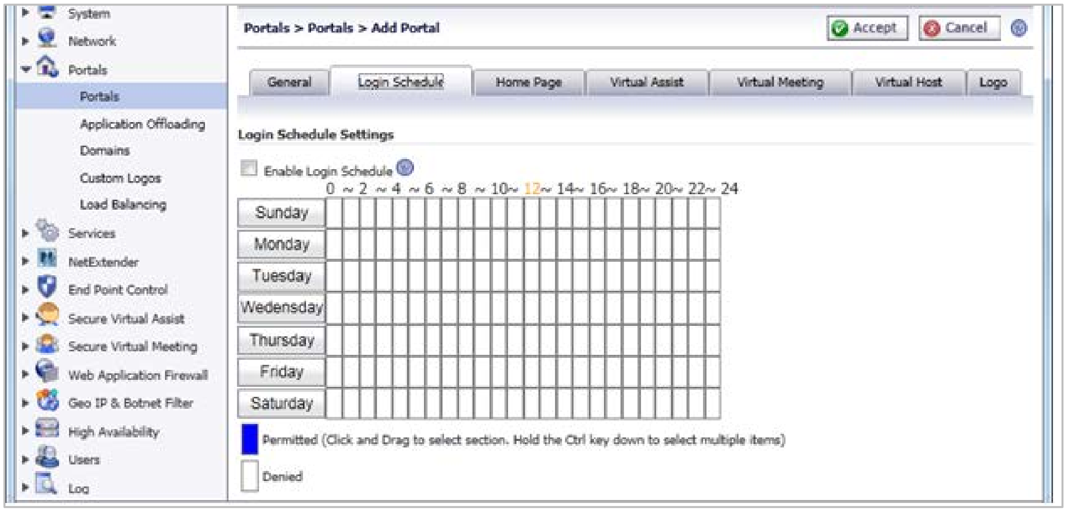
☑ Show Options Button

Home Page Message:

```
<h1>Welcome to the Dell
SonicWALL Virtual Office</h1>
<p>Dell SonicWALL's Virtual
```

- File Shares link – The File Shares main link can be set to a specific share for each portal. To configure file shares, check the **Allow File Shares on this portal** check box on the Home Page tab of the Portals > Portals > Add Portals page (shown above) and complete the related fields.

- Schedule-based Access – Access can be restricted per portal based on login time and date. Use the Portal > Login Schedule tab to create and enable a login schedule. To enable the login schedule, check the **Enable Login** Schedule check box and select the permitted login times. To select the login time, click and drag through the desired time slots, hold the **Ctrl** key while clicking time slots, or select an entire day by clicking the day.



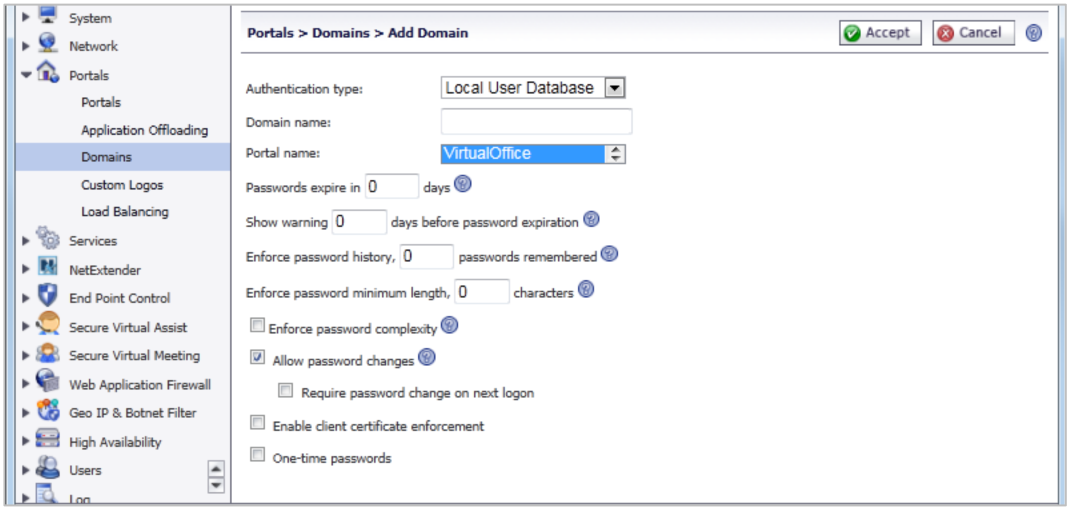
Login Schedule Settings

☐ Enable Login Schedule

■ Permitted (Click and Drag to select section. Hold the Ctrl key down to select multiple items)

□ Denied

- User Password Restrictions – Configurable passwords can be restricted on the domain level for local database users as follows:



Portals > Domains > Add Domain

Authentication type: Local User Database

Domain name:

Portal name: VirtualOffice

Passwords expire in 0 days

Show warning 0 days before password expiration

Enforce password history, 0 passwords remembered

Enforce password minimum length, 0 characters

□ Enforce password complexity

☑ Allow password changes

□ Require password change on next logon

□ Enable client certificate enforcement

□ One-time passwords

  - Same password cannot be selected for a configurable number of password changes (up to 10 changes).
  - Minimum number of characters (up to 14).
  - At least three of the following types of characters: uppercase, lowercase, base 10 digits, special characters.
  - For radius authentication users, passwords can be changed for MSCHAP/MSCHAP2 authentication protocol.  It is supported on Windows RADIUS and open source project FreeRADIUS servers, which have the additional interface for users to change password through these two protocols.

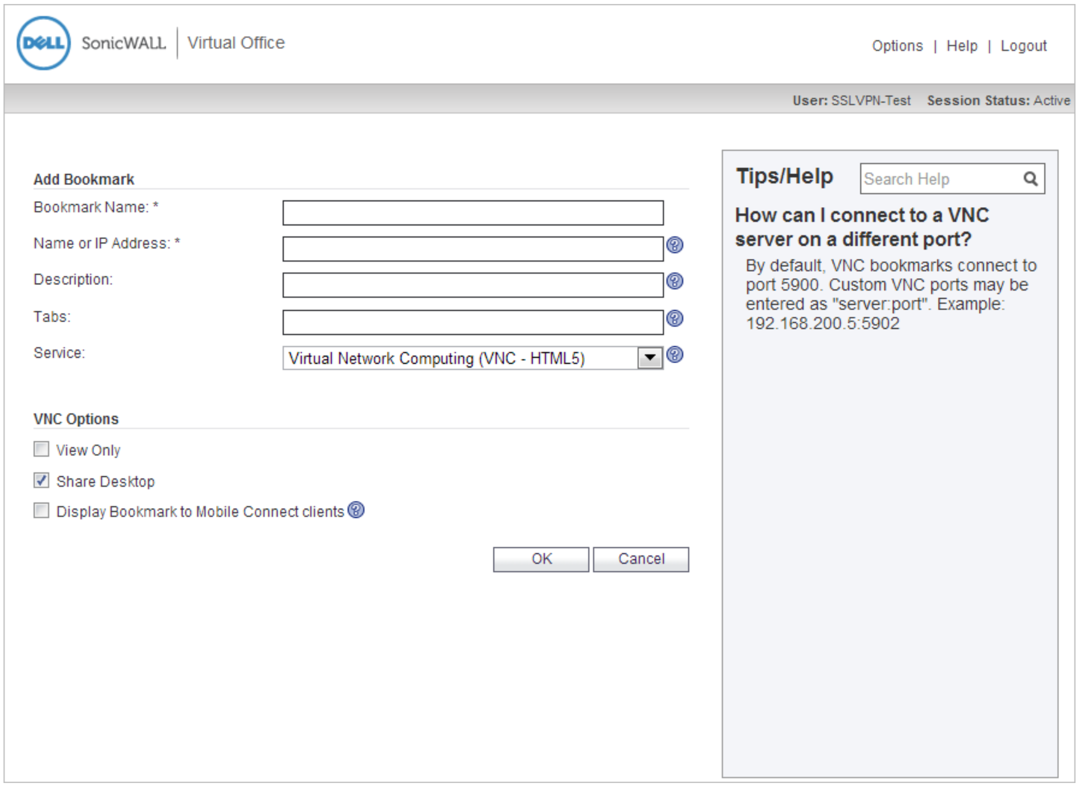
- TSRs can be generated when the appliance is rebooted and then downloaded, deleted, manually emailed, or automatically emailed (if mail settings are defined in the Log > Settings page). TSRs can also be scheduled for generation via the <sslvpn>/cgi-bin/diag settings page.
- Reverse Proxy Logging – New log entries have been created for reverse proxy logging and these log messages may be categorized by checking the **Reverse Proxy** check box on the Log > Categories page.

### *HTML5 VNC Clients*

In SRA 7.5, HTML5 clients have been added for VNC and RDP. HTML5 clients are powerful, secure clients that replace Java and ActiveX plug-ins and are supported on most browsers and mobile devices. To create an HTML5 VNC bookmark:

1. Select a user to edit on the Users > Local Users page and click the configure button.
2. On the Bookmarks tab, type in a name in the Bookmark Name field.
3. In the Name or IP Address field, enter the IP address in the server:port format (for example, 192.10.22.1:5900). By default, VNC bookmarks connect to port 5900.
4. Optionally, enter a description.
5. Optionally, in the Tabs field, type a list of comma-separated tabs where the bookmark should be located. Standard tabs do not need to be specified.
6. Select **Virtual Network Computing (VNC – HTML5)** as the Service.
7. To ignore all keyboard and mouse entries in the desktop window, select **View Only**.

8. To share the desktop between clients, select **Share Desktop**.


SonicWALL | Virtual Office
Options | Help | Logout
User: SSLVPN-Test Session Status: Active

Add Bookmark

Bookmark Name: *

Name or IP Address: *

Description:

Tabs:

Service: Virtual Network Computing (VNC - HTML5)

VNC Options

☐ View Only

☑ Share Desktop

☐ Display Bookmark to Mobile Connect clients

OK
Cancel
Tips/Help
Search Help

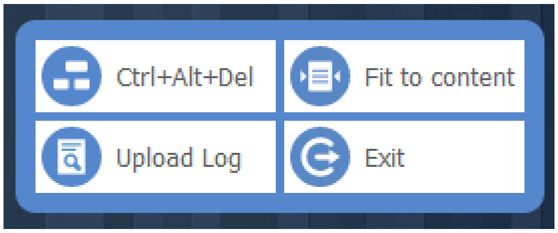
How can I connect to a VNC server on a different port?

By default, VNC bookmarks connect to port 5900. Custom VNC ports may be entered as "server:port". Example: 192.168.200.5:5902

***Note**: HTML5 VNC bookmarks can be controlled by policies defined for the Virtual Network Computing (HTML5) service. If an HTML5 VNC bookmark is blocked by a policy, the user receives a "not authorized" message.*

After an HTML5 VNC bookmark is configured, it appears as a bookmark on the Portal. When clicked, the client launches, the user is asked for a password if authentication is required by the VNC server, and the remote desktop appears.

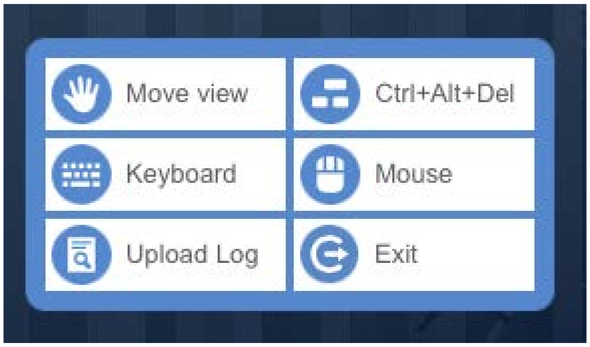
The icon shown at the top right of the window provides access to different functions, depending on whether the machine being used has a touch screen. On a machine **without** a touch screen, click the icon to display the following buttons:



Click a button to perform one of the following tasks:

| **Button** | **Click to...** |
|---|---|
| Ctrl+Alt+Del | Send the key combination input to the VNC server. |
| Fit to content | Resize the browser window to fit the content. A scroll bar is added if the content cannot be sized to fit in the window. |
| Upload Log | Upload the local logs to the SRA appliance. These logs are used for troubleshooting. |
| Exit | Close the HTML5 VNC client. |

On a machine **with** a touch screen, touch or click the icon to display the following buttons:



Click a button to perform one of the following tasks:

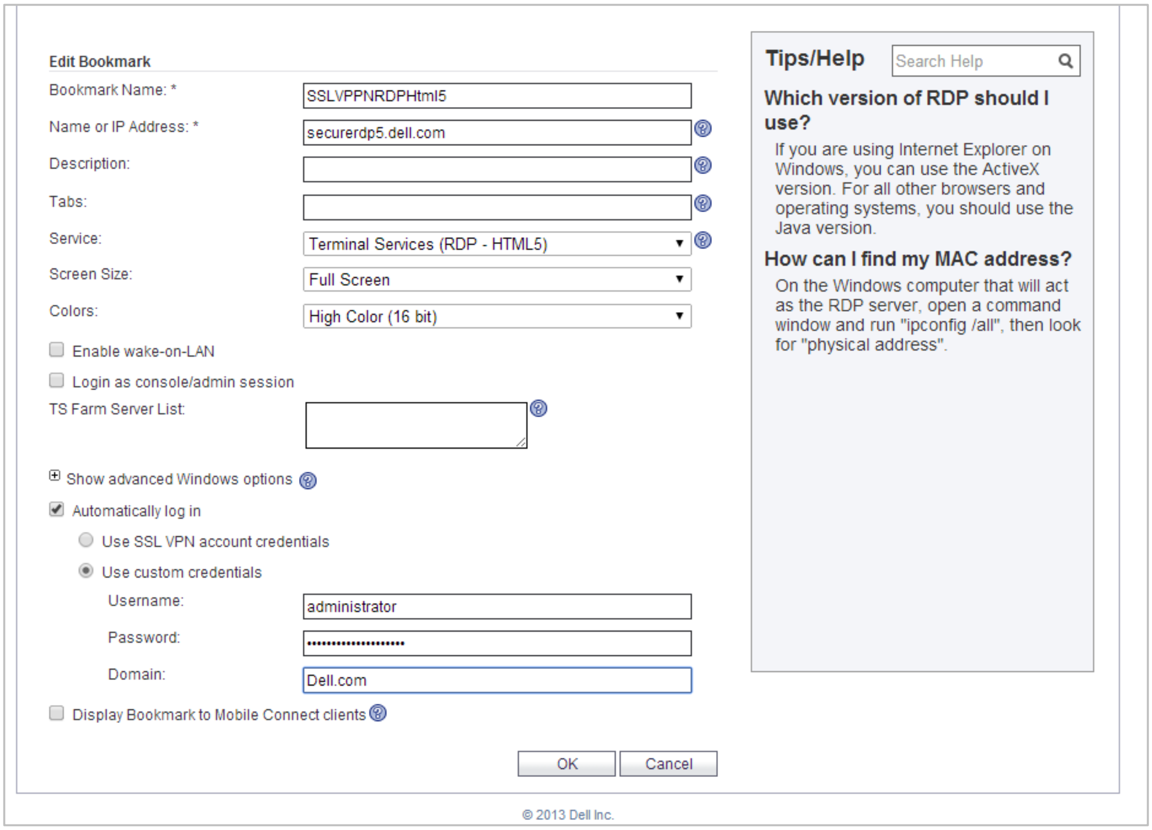
| **Button** | **Click to...** |
|---|---|
| Move view | Move the window to the desired location and click this button again to retain the new position. This function is intended for use with smaller view devices with touch screens, such as smart phones and tablets. |
| Ctrl+Alt+Del | Send the key combination input to the VNC server. |
| Keyboard | Display a virtual keyboard that can be used to input data. |
| Mouse | Change the mouse event performed when the touch screen is clicked. By default, clicking a touch screen is equivalent to clicking the left button on a mouse. Use this button to change it to simulate the right button or middle button. |
| Upload Log | Upload the local logs to the SRA appliance. These logs are used for troubleshooting. |
| Exit | Close the HTML5 VNC client. |

### *HTML5 RDP Clients*

In SRA 7.5, HTML5 clients have been added for VNC and RDP. HTML5 clients are powerful, secure clients that replace Java and ActiveX plug-ins and are supported on most browsers and mobile devices. To create an HTML5 RDP bookmark:

1. Select a user to edit on the Users > Local Users page and click the configure button.
2. On the Bookmarks tab, type in a name in the Bookmark Name field.
3. In the Name or IP Address field, enter the IP address in the server:port format (for example, 192.10.22.1:3389). By default, RDP bookmarks connect to port 3389.
4. Optionally, enter a description.
5. Optionally, in the Tabs field, type a list of comma-separated tabs where the bookmark should be located. Standard tabs do not need to be specified.
6. Select **Terminal Services (RDP – HTML5)** as the service.
7. Select the proper screen size from the drop-down list.
8. To allow single sign-on automatic login to the destination, check the **Automatically log in** check box and select the type of credentials to use.

9. To display the bookmark to Mobile Connect users, check the **Display Bookmark to Mobile Connect clients** check box.



**Edit Bookmark**

| | |
|---|---|
| Bookmark Name: * | SSLVPPNRDPHtml5 |
| Name or IP Address: * | securerdp5.dell.com |
| Description: | |
| Tabs: | |
| Service: | Terminal Services (RDP - HTML5) |
| Screen Size: | Full Screen |
| Colors: | High Color (16 bit) |

□ Enable wake-on-LAN

□ Login as console/admin session

TS Farm Server List:

⊞ Show advanced Windows options

☑ Automatically log in

○ Use SSL VPN account credentials

● Use custom credentials

| | |
|---|---|
| Username: | administrator |
| Password: | •••••••••••••••••••• |
| Domain: | Dell.com |

□ Display Bookmark to Mobile Connect clients

**Tips/Help**

**Which version of RDP should I use?**

If you are using Internet Explorer on Windows, you can use the ActiveX version. For all other browsers and operating systems, you should use the Java version.

**How can I find my MAC address?**

On the Windows computer that will act as the RDP server, open a command window and run "ipconfig /all", then look for "physical address".

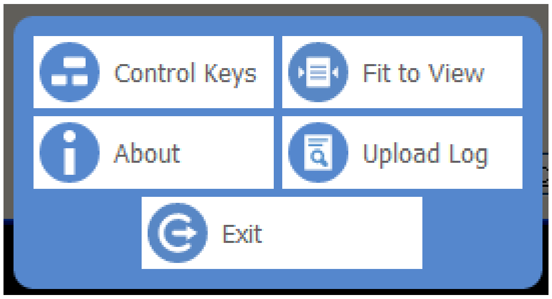
© 2013 Dell Inc.

After an HTML5 RDP bookmark is configured, it appears as a bookmark on the Portal. When clicked, the client launches, the user is asked for a password if authentication is required by the RDP server, and the remote desktop appears.

The S icon shown at the top right of the window provides access to different functions, depending on whether the machine being used has a touch screen.

### Without a touch screen:

On a machine without a touch screen, click the icon to display the following buttons:

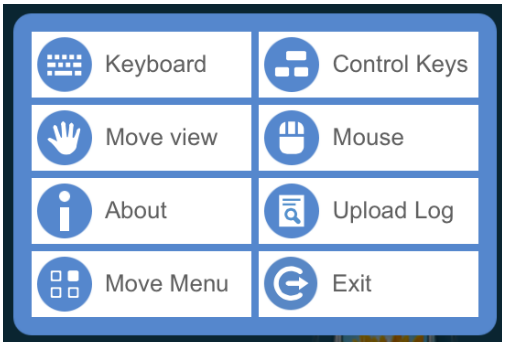


Click a button to perform one of the following tasks:

| Button | Click to... |
|---|---|
| Control Keys | Display the control keys (up arrow, Ctrl, Alt, Shift, Insert, Delete, Home, End) across the top of the screen. The up arrow hides the control keys. |
| Fit to View | Resize the content to fit the browser window. A scroll bar is added if the content cannot be sized to fit in the window. |
| About | Display information about the Dell SonicWALL Secure Remote Desktop. |
| Upload Log | Upload the local logs to the SRA appliance. These logs are used for troubleshooting. |
| Exit | Close the HTML5 RDP client. |

**With a touch screen:**

On a machine with a touch screen, touch or click the icon to display the following buttons:



Click a button to perform one of the following tasks:

| Button | Click to... |
|---|---|
| Keyboard | Display a virtual keyboard that can be used to input data. |
| Control Keys | Display the control keys (up arrow, Ctrl, Alt, Shift, Insert, Delete, Home, End) across the top of the screen. The up arrow hides the control keys. |
| Move view | Move the window to the desired location and click this button again to retain the new position. This function is intended for use with smaller view devices with touch screens, such as smart phones and tablets. |
| Mouse | Change the mouse event performed when the touch screen is clicked. By default, clicking a touch screen is equivalent to clicking the left button on a mouse. Use this button to change it to simulate the right button or middle button. |
| About | Display information about the Dell SonicWALL Secure Remote Desktop. |
| Upload Log | Upload the local logs to the SRA appliance. These logs are used for troubleshooting. |
| Move Menu | Move the S icon to a different corner of the window. |
| Exit | Close the HTML5 RDP client. |

### Large touch screen:

For devices with large touch screens, a panel is displayed. Button functions are the same except for:

- The up arrow is used to hide the panel and display the setting menu icon.
- The mouse button is stateful. That is, if the left button is blue, clicking the device is regarded as a left click. Otherwise, the click is regarded as right click. The state of the button can be switched by clicking the mouse button.

### External keyboards on touch devices:

Input from an external keyboard is recognized only when the keyboard icon is on (blue).

**Exception**: There is no keyboard icon on Internet Explorer 10 on desktop mode for Surface. The input of external keyboard is always sent to the HTML5 RDP client.

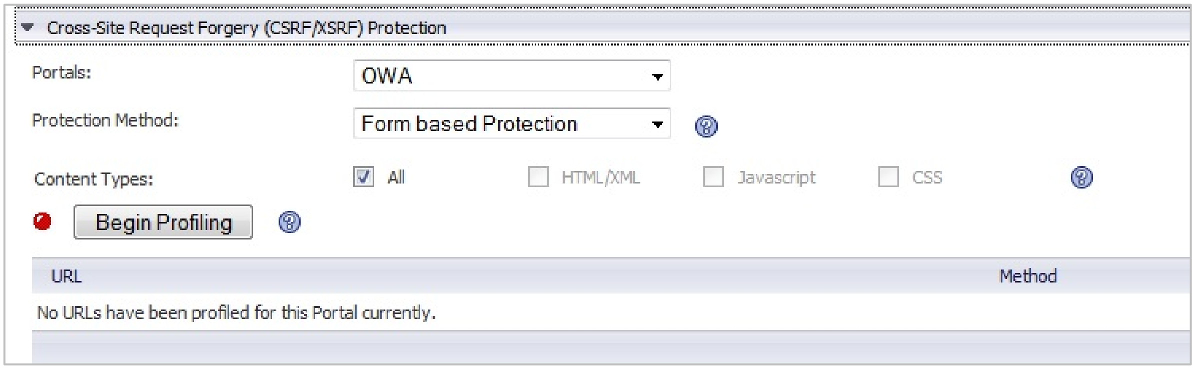
### Pinch to zoom:

The RDP client can be pinched to zoom on touch devices.

## *WAF Enhancements*

Web Application Firewall now supports form-based CSRF protection, which is faster and offers less false positives. Perform the following steps to configure and monitor form-based CSRF protection:

1. Navigate to the Web Application Firewall > Settings page and click **Cross-Site Request Forgery (CSRF/XSRF) Protection** to expand it.



Cross-Site Request Forgery (CSRF/XSRF) Protection

Portals: OWA

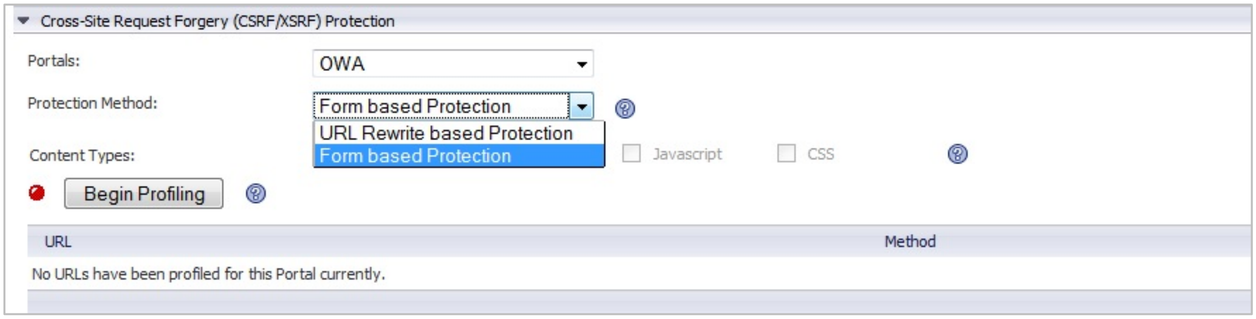
Protection Method: Form based Protection

Content Types: ☑ All □ HTML/XML □ Javascript □ CSS

Begin Profiling

| URL | Method |
|---|---|
| No URLs have been profiled for this Portal currently. | |

2. Select **Form based Protection** from the **Protection Method** drop-down list, which displays protection modes. (Selecting URL Rewrite based Protection uses the method used in previous SRA releases.)



Cross-Site Request Forgery (CSRF/XSRF) Protection

Portals: OWA

Protection Method: Form based Protection

URL Rewrite based Protection

Form based Protection

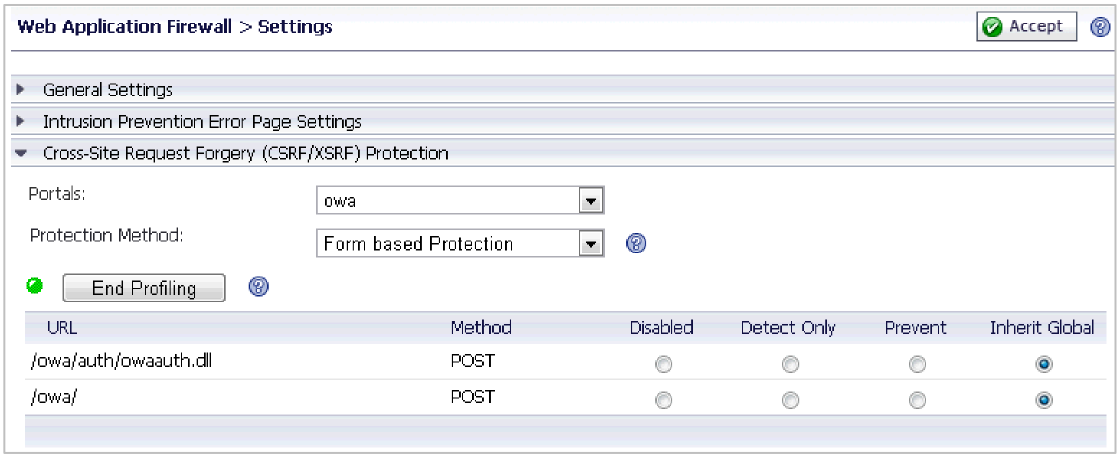
Content Types: □ Javascript □ CSS

Begin Profiling

| URL | Method |
|---|---|
| No URLs have been profiled for this Portal currently. | |

3. The **Protection Method** options are greyed out only when **URL Rewrite based Protection** is selected and accepted. To change the mode to **Form based Protection**, select it from the drop-down list and click **Accept**.
4. After selecting a Protection Method, click the **Begin Profiling** button.

5. Open a browser to access the portal. Do as many operations as possible so the actions can be profiled and configured under CRF protection. After profiling for a while, a URL list is generated and displayed on the Web Application Firewall > Settings page.



Web Application Firewall > Settings
Accept
General Settings
Intrusion Prevention Error Page Settings
Cross-Site Request Forgery (CSRF/XSRF) Protection
End Profiling

Portals: owa

Protection Method: Form based Protection

| URL | Method | Disabled | Detect Only | Prevent | Inherit Global |
|---|---|---|---|---|---|
| /owa/auth/owaauth.dll | POST | ○ | ○ | ○ | ● |
| /owa/ | POST | ○ | ○ | ○ | ● |

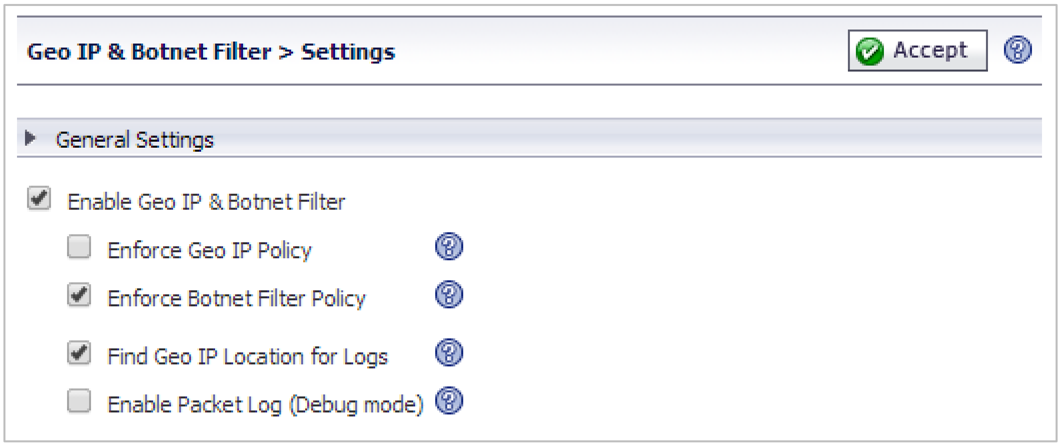
When enabled and a potential CSRF attack is detected (whether a CSRF token is wrong or missing), it displays an error page and is logged by SRA.

Optionally, different actions can be configured for different URLs. After making configuration changes, click **End Profiling** to prevent a potential CSRF attack from jeopardizing protection.

## *Geo IP and Botnet Filter Enhancements*

The following Geo IP and Botnet Filter enhancements have been added to SRA 7.5:

- General Settings redesigned – A new design of the General Settings tab on the Geo IP & Botnet Filter > Settings page is introduced to avoid misunderstanding of the options. The functionality of the options is the same as in the previous SRA release. Corresponding tool tips are also added.



☑ Enable Geo IP & Botnet Filter

□ Enforce Geo IP Policy

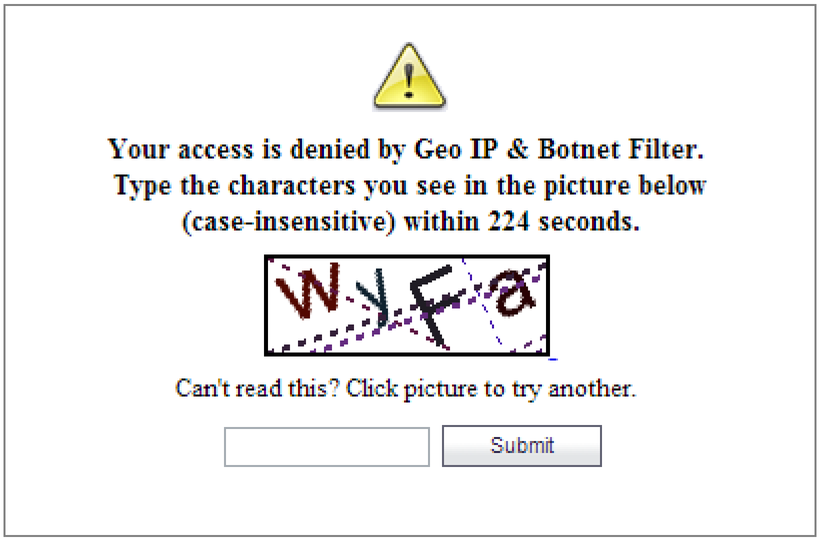
☑ Enforce Botnet Filter Policy

☑ Find Geo IP Location for Logs

□ Enable Packet Log (Debug mode)

- Remediation using CAPTCHA – Access to an SRA appliance from aggressive IP addresses is denied when Geo IP & Botnet Filter is enabled. Remediation provides valid users an opportunity to establish their validity and gain access.

  For web access, users are redirected to the CAPTCHA page, as shown below. A countdown timer tells the time that remains for the user to enter the letters shown in the picture. The user must finish remediation within the time limit, otherwise the IP address is added to the block list and all access from that IP address is blocked for a period of time.

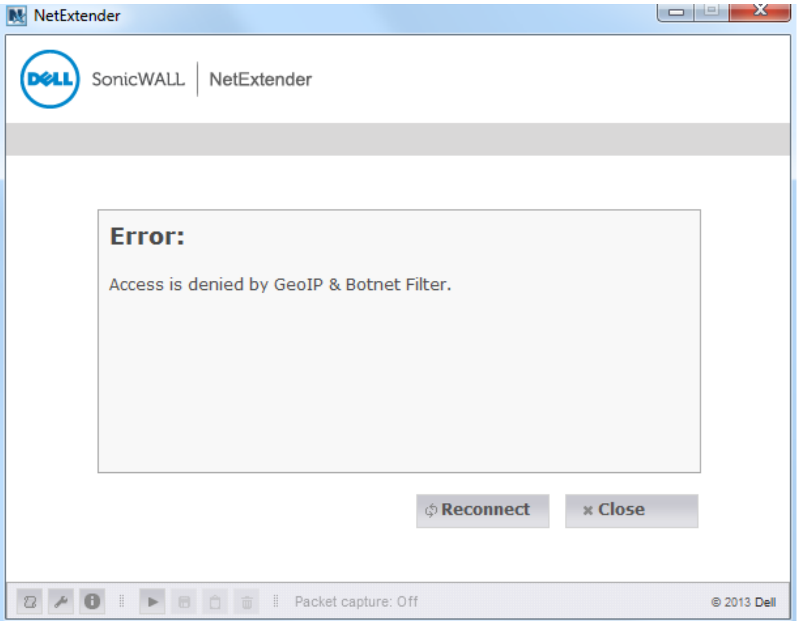


Your access is denied by Geo IP & Botnet Filter.
Type the characters you see in the picture below
(case-insensitive) within 224 seconds.

Can't read this? Click picture to try another.

If remediation is successful within the allowed time, the user is directed to the web page that was requested.

For client access to the SRA appliance, such as NetExtender, Virtual Meeting, or Virtual Assist, a message is displayed in the client window and then a browser window is automatically opened to display the CAPTCHA picture and entry field.

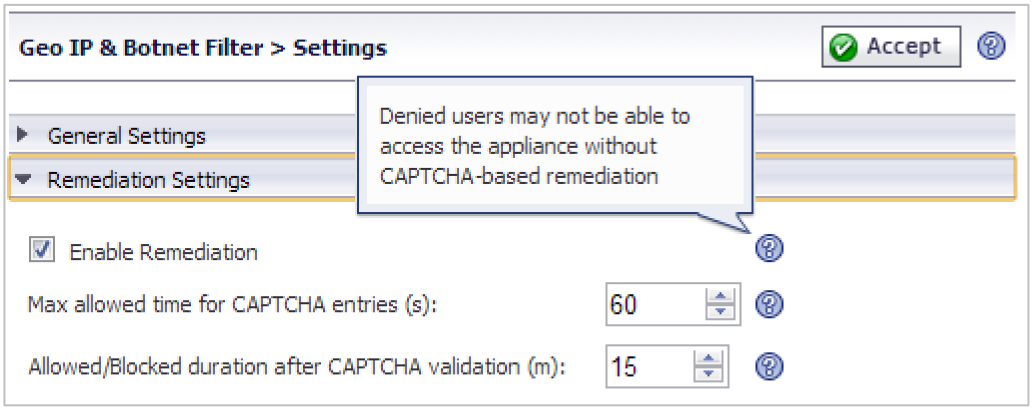


**Error:**

Access is denied by GeoIP & Botnet Filter.

During the valid duration, all access from the IP address is allowed. After the duration expires, access is not interrupted for users who are still logged in, but remediation is required again after the user logs out.

Related settings for remediation are available on the Geo IP & Botnet Filter > Settings page in the SRA appliance management interface.



**Geo IP & Botnet Filter > Settings**

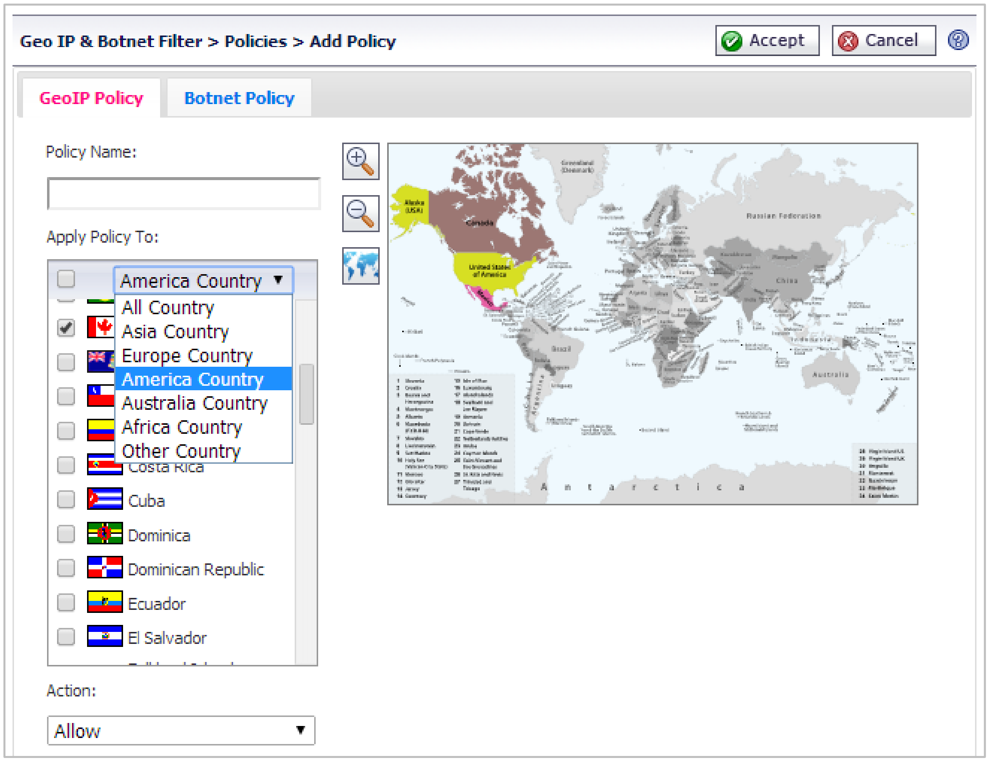
Denied users may not be able to access the appliance without CAPTCHA-based remediation

☑ Enable Remediation

Max allowed time for CAPTCHA entries (s): 60

Allowed/Blocked duration after CAPTCHA validation (m): 15

- Geo IP Policies with map – The Geo IP & Botnet Filter > Policies page in management interface is reorganized with separate tabs for Geo IP access policies and Botnet access policies. The Geo IP policies page includes a world map. When creating a policy, you can click on countries in the map to select or clear them, or you can select/clear them by clicking the checkbox in the list. On the map, unselected countries display in grey and selected countries display in color. In the list, a drop-down list is provided with countries grouped together into continents for convenient selection of all countries belonging to a continent.



**Geo IP & Botnet Filter > Policies > Add Policy**

Policy Name:

Apply Policy To:

□ America Country ▾

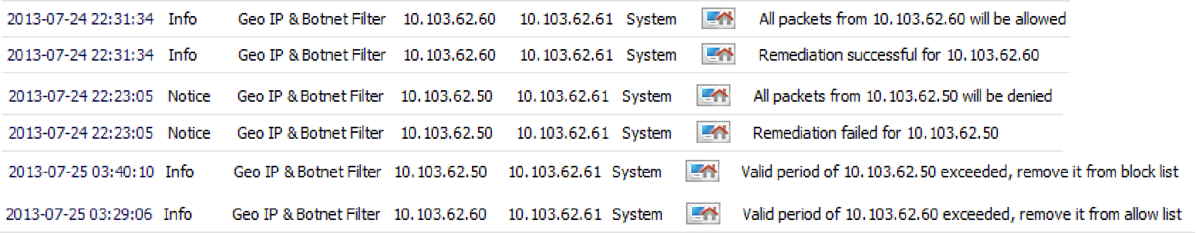
All Country
Asia Country
Europe Country
America Country
Australia Country
Africa Country
Other Country

☑
□
□
□
□ Costa Rica
□ Cuba
□ Dominica
□ Dominican Republic
□ Ecuador
□ El Salvador

Action:

Allow ▾

- Successful and Failed remediation messages –Successful messages show a log level of Info, and Failed messages show a log level of Notice. A log message is also generated for a user after a CAPTCHA session expires, regardless of whether remediation failed or succeeded.

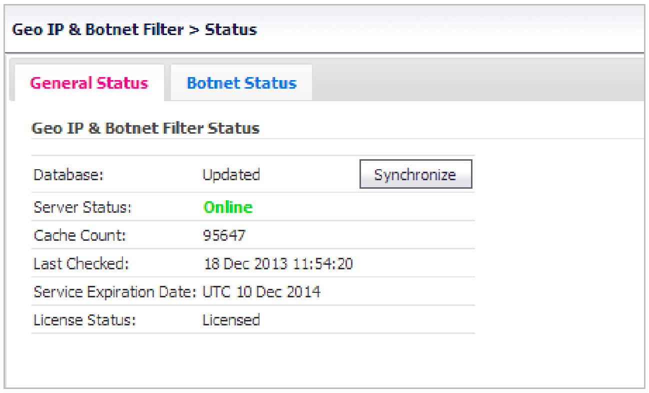


```
2013-07-24 22:31:34  Info    Geo IP & Botnet Filter  10.103.62.60  10.103.62.61  System  All packets from 10.103.62.60 will be allowed
2013-07-24 22:31:34  Info    Geo IP & Botnet Filter  10.103.62.60  10.103.62.61  System  Remediation successful for 10.103.62.60
2013-07-24 22:23:05  Notice  Geo IP & Botnet Filter  10.103.62.50  10.103.62.61  System  All packets from 10.103.62.50 will be denied
2013-07-24 22:23:05  Notice  Geo IP & Botnet Filter  10.103.62.50  10.103.62.61  System  Remediation failed for 10.103.62.50
2013-07-25 03:40:10  Info    Geo IP & Botnet Filter  10.103.62.50  10.103.62.61  System  Valid period of 10.103.62.50 exceeded, remove it from block list
2013-07-25 03:29:06  Info    Geo IP & Botnet Filter  10.103.62.60  10.103.62.61  System  Valid period of 10.103.62.60 exceeded, remove it from allow list
```

- The **Find Geo IP Location for Logs** option has been added. When this option is enabled, Geo location tags are added to most of the logs generated by the appliance for EPC, WAF and others.

- The **Enable Packet Log (Debug mode)** option has been added and when enabled, logs are generated for all allowed and denied packets through Geo IP.

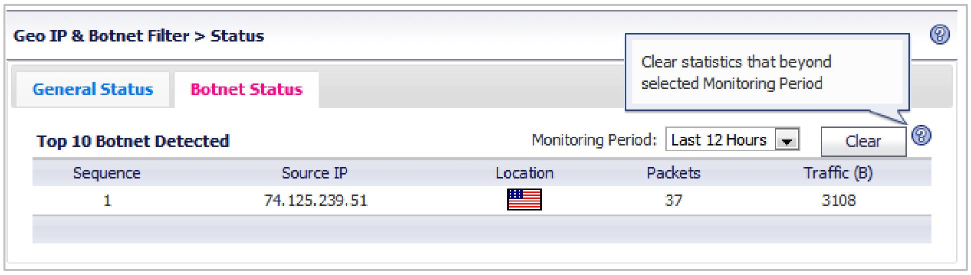
- Cache management has been removed, since caches are managed automatically by the server. Therefore, cache management settings have been removed from the Geo IP and Botnet Filter > Settings page, and the **Offline Mode** and **Clear All** buttons have been replaced by a **Synchronize** button on the Geo IP and Botnet Filter > Status page. Clicking **Synchronize** instructs the server to immediately check for an update from the backend server.



Geo IP & Botnet Filter > Status
General Status
Botnet Status
Geo IP & Botnet Filter Status
Synchronize

| | |
|---|---|
| Database: | Updated |
| Server Status: | Online |
| Cache Count: | 95647 |
| Last Checked: | 18 Dec 2013 11:54:20 |
| Service Expiration Date: | UTC 10 Dec 2014 |
| License Status: | Licensed |

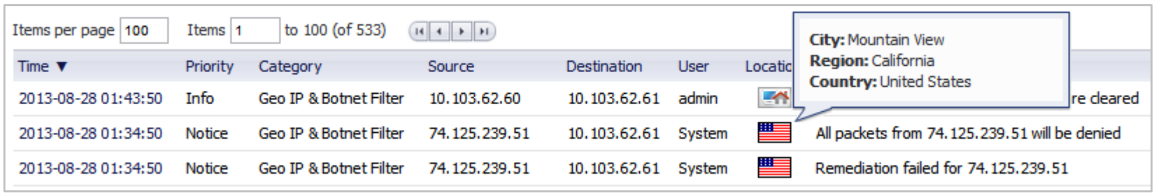
- Clear Botnet Statistics – A **Clear** button and Monitoring Period drop-down list have been added to the Geo IP & Botnet Filter page to clear aged Botnet statistics. Select the monitoring period and click **Clear** to remove all statistics older than the selected period. When prompted to confirm removal, click **OK**.



Geo IP & Botnet Filter > Status
General Status
Botnet Status
Clear statistics that beyond selected Monitoring Period
Top 10 Botnet Detected
Monitoring Period: Last 12 Hours
Clear

| Sequence | Source IP | Location | Packets | Traffic (B) |
|---|---|---|---|---|
| 1 | 74.125.239.51 | | 37 | 3108 |

- Geographic Location – Pages with a Location column now contain a mouse-over popup showing the originating city and IP address, if available.



City: Mountain View
Region: California
Country: United States

| Time ▼ | Priority | Category | Source | Destination | User | Locatic | |
|---|---|---|---|---|---|---|---|
| 2013-08-28 01:43:50 | Info | Geo IP & Botnet Filter | 10.103.62.60 | 10.103.62.61 | admin | | re cleared |
| 2013-08-28 01:34:50 | Notice | Geo IP & Botnet Filter | 74.125.239.51 | 10.103.62.61 | System | | All packets from 74.125.239.51 will be denied |
| 2013-08-28 01:34:50 | Notice | Geo IP & Botnet Filter | 74.125.239.51 | 10.103.62.61 | System | | Remediation failed for 74.125.239.51 |

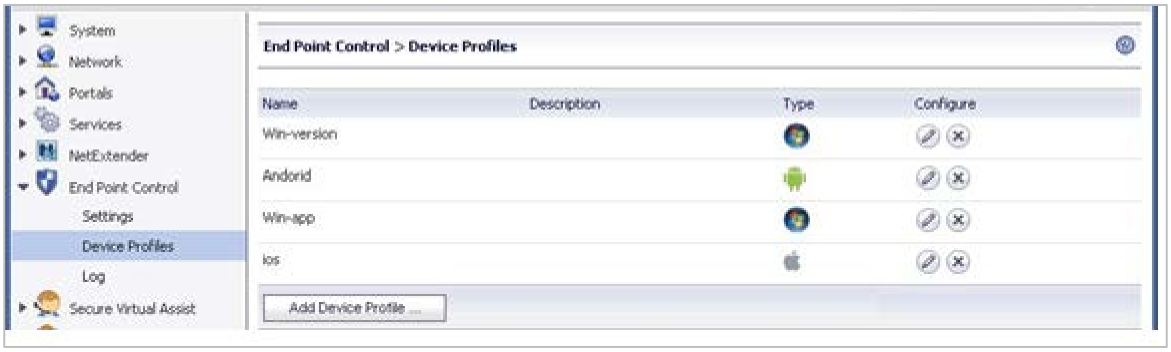
## *EPC Enhancements*

Mobile Connect allows iOS and Android users to securely access their networks from a mobile device.  EPC has been integrated into the Mobile Connect application to provide security protection from threats against client mobile devices and protect the SRA appliance from threats originating from these mobile devices. This integration allows EPC checking before allowing login to the SSLVPN appliance.

***Note**:  AntiVirus and personal firewall applications on Android mobile devices require OESIS support.*

Integrating EPC with Mobile Connect affects the following SRA Management Console pages:

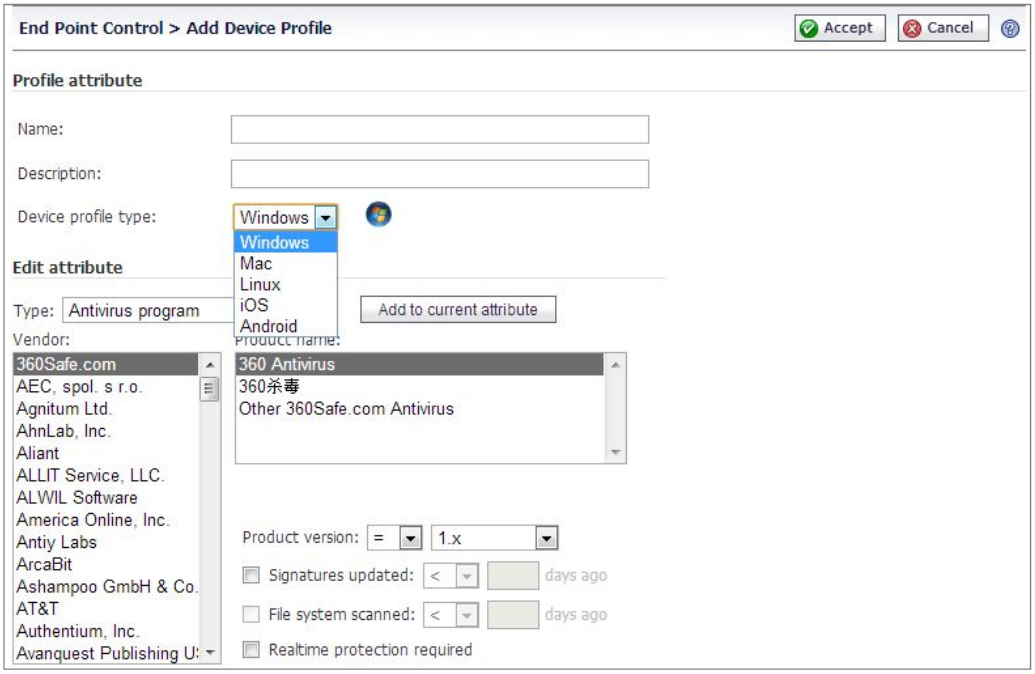
- End Point Control > Device Profiles – Android and iOS have been added to the list to provide access to configuration pages.



End Point Control > Device Profiles

| Name | Description | Type | Configure |
|---|---|---|---|
| Win-version | | | |
| Andorid | | | |
| Win-app | | | |
| ios | | | |

- End Point Control > Add/Edit Device Profile – The Add/Edit Device Profile page has been modified to include Android and iOS mobile device configuration options.



End Point Control > Add Device Profile

Profile attribute

Name:

Description:

Device profile type: Windows

Edit attribute

Type: Antivirus program

Vendor: 360Safe.com, AEC, spol. s r.o., Agnitum Ltd., AhnLab, Inc., Aliant, ALLIT Service, LLC., ALWIL Software, America Online, Inc., Antiy Labs, ArcaBit, Ashampoo GmbH & Co., AT&T, Authentium, Inc., Avanquest Publishing U:

Product name: 360 Antivirus, 360杀毒, Other 360Safe.com Antivirus

Product version: = 1.x

□ Signatures updated: < days ago

□ File system scanned: < days ago

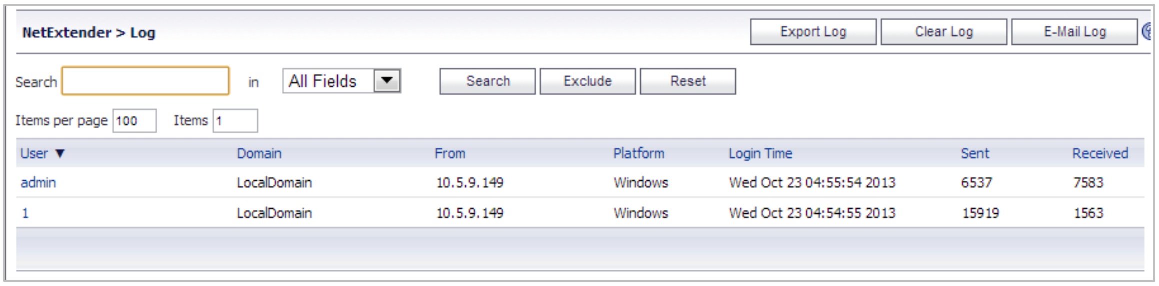
□ Realtime protection required

- When an EPC check fails, an EPC check failed message is added to the alert dialog.

## NetExtender Enhancements

The following NetExtender enhancements have been added to SRA 7.5:

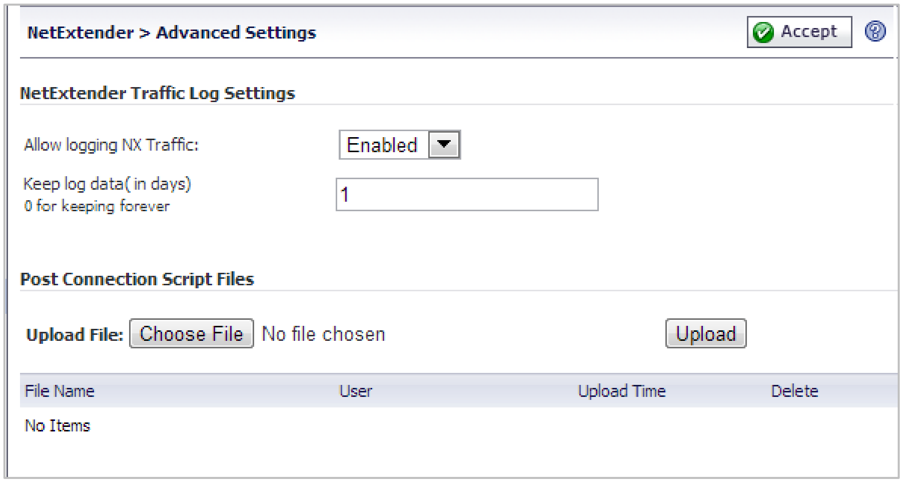
- NetExtender Traffic Logging – The NetExtender > Log page now shows traffic summary information, destination IP address and port, type of traffic, and sent/received data size. Click the User heading to expand the view to also display the Port and Protocol.



Items per page 100 Items 1

| User ▼ | Domain | From | Platform | Login Time | Sent | Received |
|---|---|---|---|---|---|---|
| admin | LocalDomain | 10.5.9.149 | Windows | Wed Oct 23 04:55:54 2013 | 6537 | 7583 |
| 1 | LocalDomain | 10.5.9.149 | Windows | Wed Oct 23 04:54:55 2013 | 15919 | 1563 |

Use the **Allow logging NX Traffic** field on the NetExtender > Extend Settings page to enable or disable traffic logging. Use the **Keep log data** field to specify how long to keep log data.


NetExtender > Advanced Settings
Accept
NetExtender Traffic Log Settings
Post Connection Script Files
Upload File:
Choose File
Upload

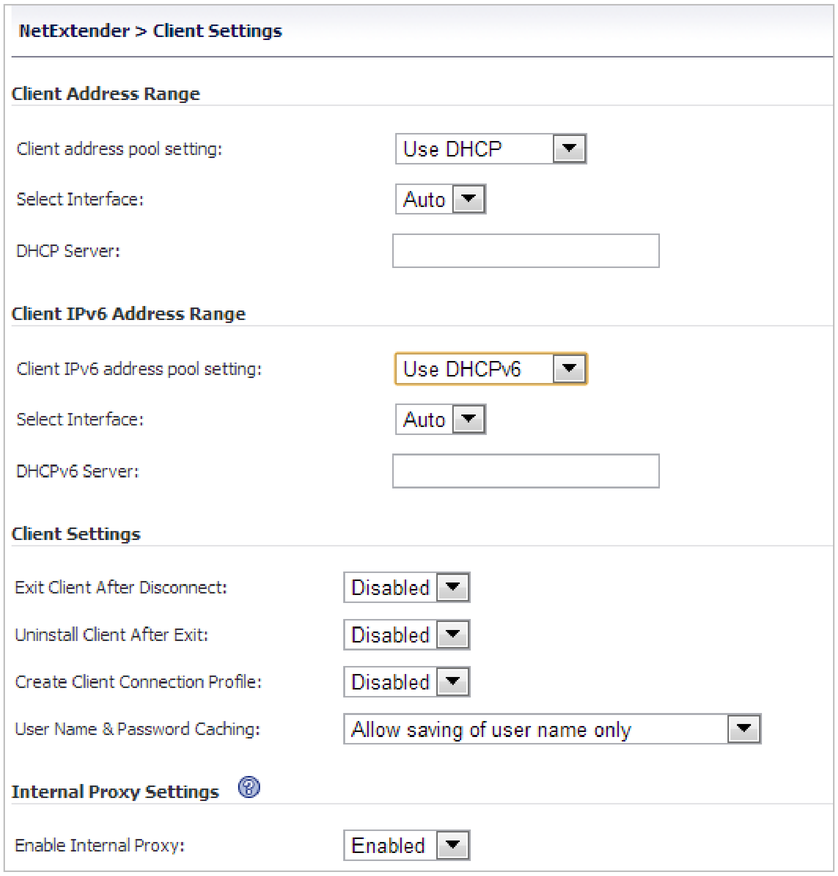
Allow logging NX Traffic: Enabled

Keep log data( in days) 1
0 for keeping forever

No file chosen

| File Name | User | Upload Time | Delete |
|---|---|---|---|
| No Items | | | |

- DHCP Support for NetExtender Client IPv4/IPv6 Addresses – DHCP/DHCPv6 can now manage NetExtender client IPv4/IPv6 addresses along with other IPv4/IPv6 addresses in the LAN, which minimizes IP conflicts. Similar to configuring a static pool, DHCP/DHCPv6 can be configured at the global policies, local group, or local user level using the NetExtender > Client Settings page, Users > Local Groups > Edit Global Policies, or Users > Local Users > Edit Global Policies pages.



**NetExtender > Client Settings**

**Client Address Range**

Client address pool setting: Use DHCP

Select Interface: Auto

DHCP Server:

**Client IPv6 Address Range**

Client IPv6 address pool setting: Use DHCPv6

Select Interface: Auto

DHCPv6 Server:

**Client Settings**

Exit Client After Disconnect: Disabled

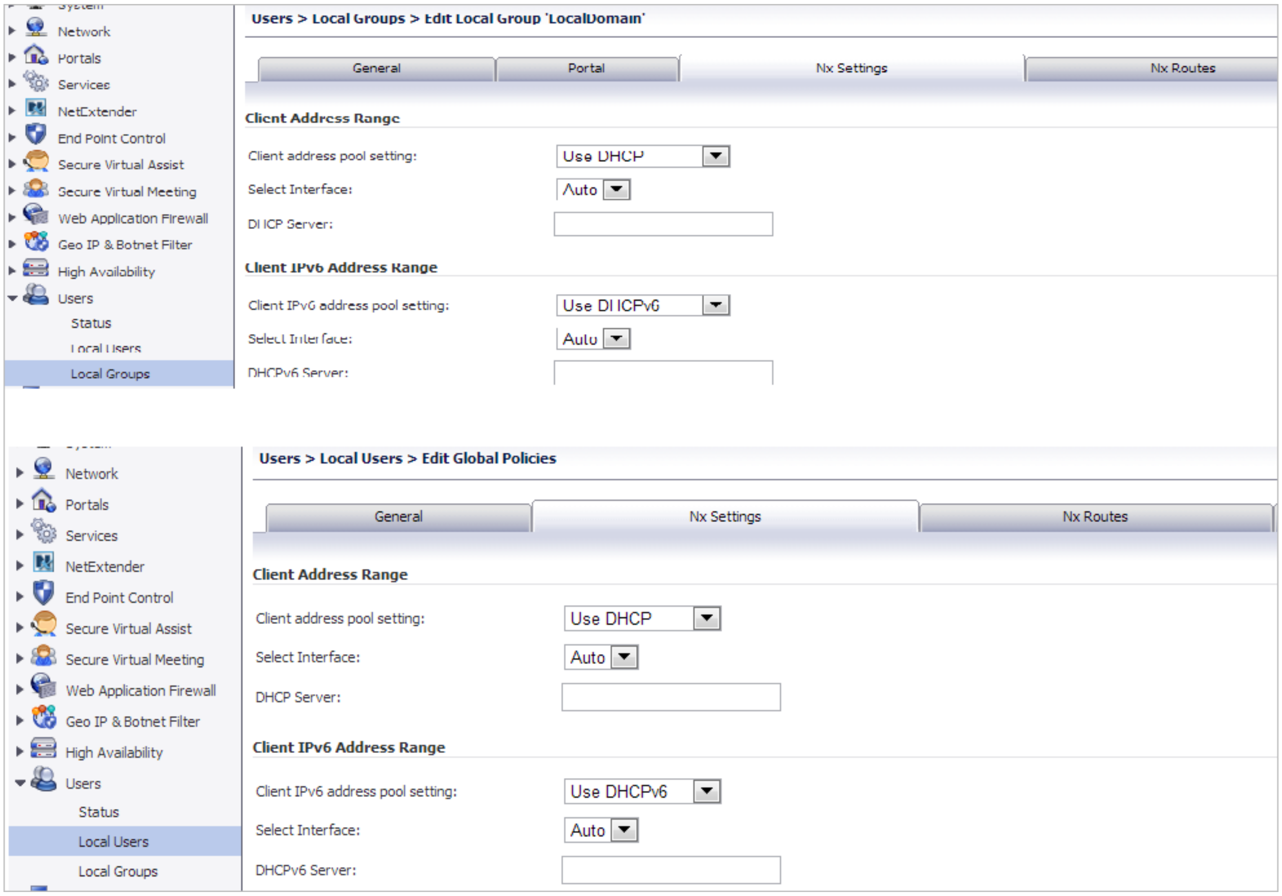
Uninstall Client After Exit: Disabled

Create Client Connection Profile: Disabled

User Name & Password Caching: Allow saving of user name only

**Internal Proxy Settings**

Enable Internal Proxy: Enabled



Users > Local Groups > Edit Local Group 'LocalDomain'

Client Address Range

Client address pool setting: Use DHCP

Select Interface: Auto

DHCP Server:

Client IPv6 Address Range

Client IPv6 address pool setting: Use DHCPv6

Select Interface: Auto

DHCPv6 Server:

Users > Local Users > Edit Global Policies

Client Address Range

Client address pool setting: Use DHCP

Select Interface: Auto

DHCP Server:

Client IPv6 Address Range

Client IPv6 address pool setting: Use DHCPv6

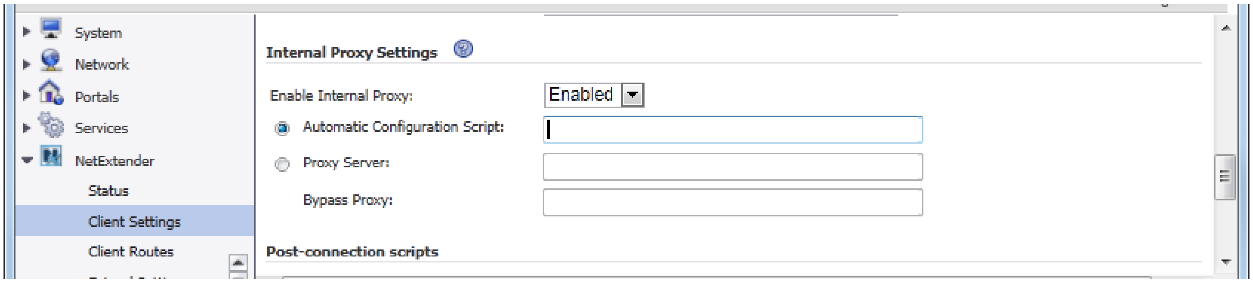
Select Interface: Auto

DHCPv6 Server:

After selecting **Use DHCP**, select **Auto** or a specific interface from the **Select Interface** drop-down list. To dynamically allocate IP addresses from a DHCP server, enter its IP address in the **DHCP server** field. If nothing is specified, the appliance sends broadcast requests to locate DHCP servers that can allocate addresses.

- Internal Proxy Settings – In SRA 7.5, NetExtender traffic can be proxied to an internal proxy server in addition to the NetExtender client being able to set a proxy for an external network. And, a configuration script can be pushed automatically upon connection. To set the internal proxy:

  1. In the NetExtender > Client Settings page select **Enabled** in the Enable Internal Proxy drop-down list.
  2. To automatically execute a configuration script that sets the internal proxy, select the **Automatic Configuration Script** radio button and then type the path and file name.
  3. Select the **Proxy Server** radio button, and type the host that will be bypassed to the proxy server.



Internal Proxy Settings

Enable Internal Proxy: Enabled

● Automatic Configuration Script:

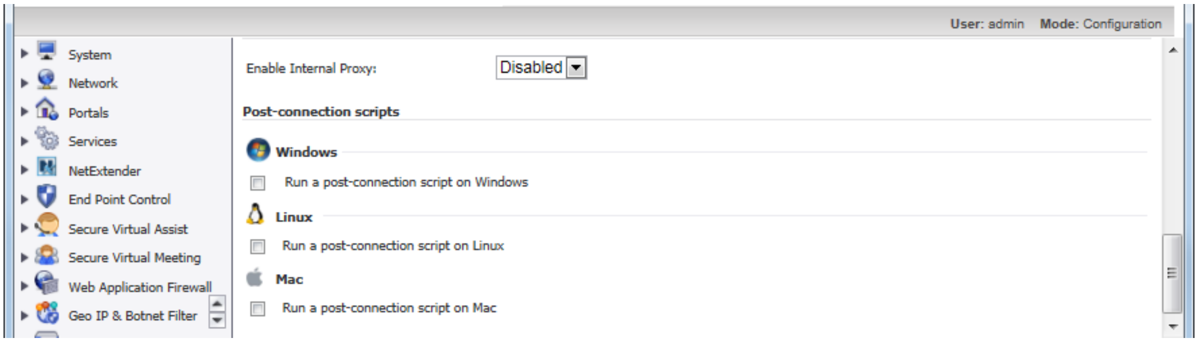
○ Proxy Server:

Bypass Proxy:

Post-connection scripts

After NetExtender is connected, internal proxy settings are pushed to the client side and the proxy is set for the Dell SonicWALL NetExtender virtual adapter.

- Post Connection Script – A script can be set to automatically run after connection. To configure this feature, on the NetExtender > Client Settings page configure the internal proxy and check the **Run a post-connection script** check box for Windows, Linux, or Mac.



Enable Internal Proxy: Disabled

Post-connection scripts

Windows

□ Run a post-connection script on Windows

Linux

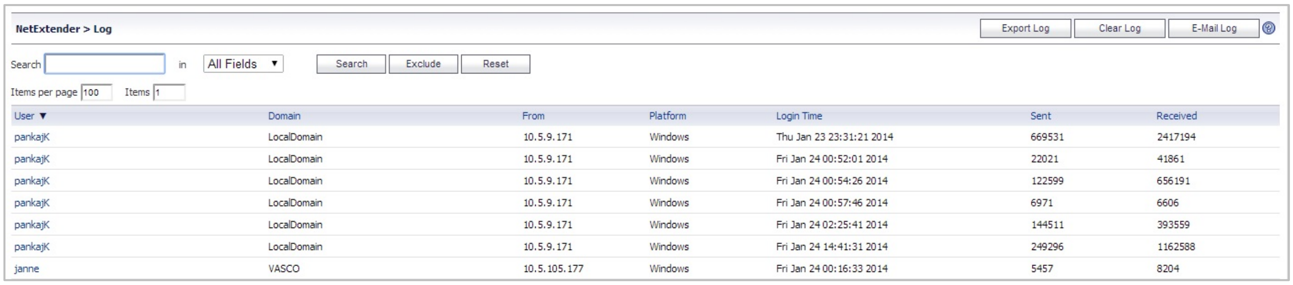
□ Run a post-connection script on Linux

Mac

□ Run a post-connection script on Mac

- Login scripts can be pushed from the SRA appliance to connecting NetExtender clients. Instead of configuring per-user login scripts at the endpoint as in previous versions, a script can be created on the appliance and pushed to connecting users based on user, group, or global control policies.

- Destination IP address of internal resources accessed by NetExtender is now displayed on the NetExtender > Log page.



Search [ ] in All Fields

Items per page 100 Items 1

| User ▼ | Domain | From | Platform | Login Time | Sent | Received |
|---|---|---|---|---|---|---|
| pankajK | LocalDomain | 10.5.9.171 | Windows | Thu Jan 23 23:31:21 2014 | 669531 | 2417194 |
| pankajK | LocalDomain | 10.5.9.171 | Windows | Fri Jan 24 00:52:01 2014 | 22021 | 41861 |
| pankajK | LocalDomain | 10.5.9.171 | Windows | Fri Jan 24 00:54:26 2014 | 122599 | 656191 |
| pankajK | LocalDomain | 10.5.9.171 | Windows | Fri Jan 24 00:57:46 2014 | 6971 | 6606 |
| pankajK | LocalDomain | 10.5.9.171 | Windows | Fri Jan 24 02:25:41 2014 | 144511 | 393559 |
| pankajK | LocalDomain | 10.5.9.171 | Windows | Fri Jan 24 14:41:31 2014 | 249296 | 1162588 |
| janne | VASCO | 10.5.105.177 | Windows | Fri Jan 24 00:16:33 2014 | 5457 | 8204 |

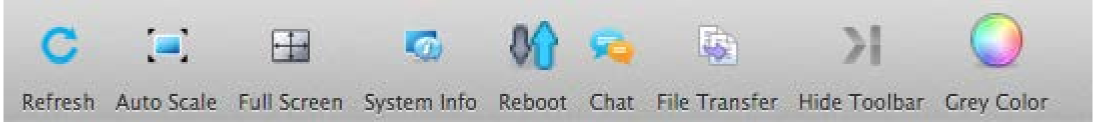
## Secure Virtual Assist and Access Enhancements

Beginning in SRA 7.5 Secure Virtual Assist technician mode is supported on MacOS. (In previous versions, only the customer mode was supported on MacOS.

To configure Secure Virtual Assist for MacOS:

1. In the Proxy Settings tab, either load proxy settings from the system configuration by clicking **the Load System Proxy Settings** button or manually configure the proxy server, port, bypassed proxy, user name, and password.
2. In the Connection Profiles tab, view and manage connection profiles.
3. In the Connection Settings tab, create and edit connection profiles:
   - When **Auto View Only** is enabled, any mouse or keyboard action while a technician is connected triggers the View Only mode. When **Active Mode** is enabled, users are in Active mode by default while a technician is connected.
   - When **Full Color** is selected and the user is in View Only mode, the technician view is in full color. When **Gray Scale** is selected, the view is grey monochrome.

MacOS Secure Virtual Assist windows and toolbar are very similar to the Windows version, which are explained in detail in the *Dell SonicWALL SRA User Guide*.



The toolbar contains the following actions:

- Refresh – Refresh the entire screen frame.
- Auto Scale – Adjust the screen viewer to fit the window size.
- Full Screen – Place the screen view in full screen mode.
- System info – Show the system information for the machine.
- Reboot – Reboot the machine.
- Chat – Text chat with user.
- File Transfer – Transfer files/Directories between technician and users.
- Hide Toolbar – Hide the toolbar.

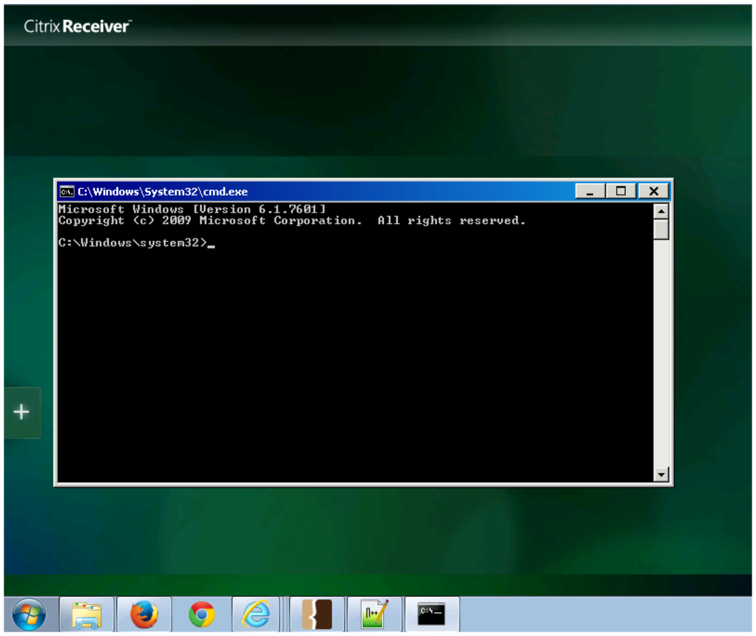
## *Secure Virtual Office Enhancement*

The Active Directory user object "usePrincipalName" can now be used to log in to Secure Virtual Office.

## *Bookmark Enhancements*

The following bookmark enhancements are included in SRA 7.5:

- Citrix bookmarks support Citrix XenApp 6.5.



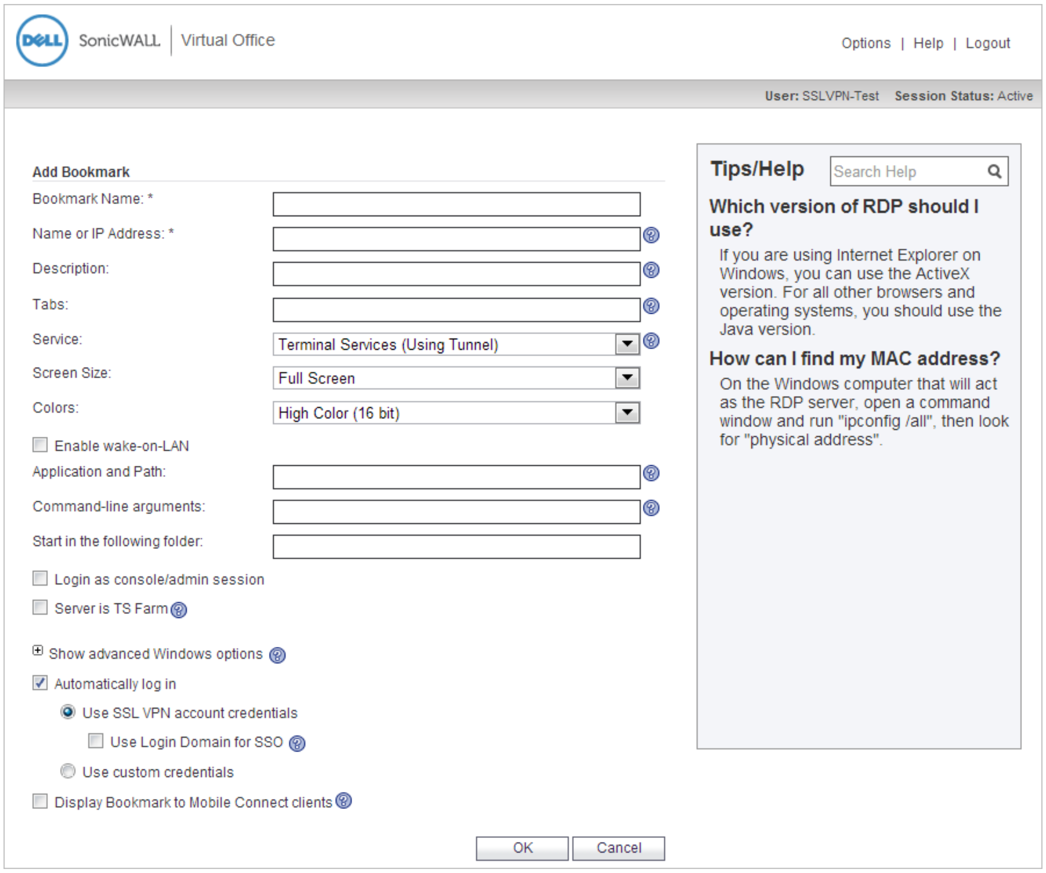
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>_
```

- Verbose logging for HTTP/HTTPS backend connections can be turned on by enabling the **Reverse Proxy** category under Log > Categories. This provides useful troubleshooting information for reverse proxy connections with the backend server.

### *RDP Over NetExtender*

To support Windows 8, SRA 7.5 includes a new Terminal Services bookmark that uses NetExtender to tunnel Remote Desktop Protocol (RDP) data. It is configured and appears like existing RDP bookmarks, except a Terminal Services bookmark starts NetExtender before launching the native RDC client. Therefore, it needs a NetExtender connection allowed to the portal, but no longer needs an RDP browser plug-in.

To create a Terminal Services bookmark that uses a tunnel, select **Terminal Services (Using Tunnel)** as the Service on the Add Bookmark page.



**User:** SSLVPN-Test **Session Status:** Active

**Add Bookmark**

Bookmark Name: *

Name or IP Address: *

Description:

Tabs:

Service: Terminal Services (Using Tunnel)

Screen Size: Full Screen

Colors: High Color (16 bit)

□ Enable wake-on-LAN

Application and Path:

Command-line arguments:

Start in the following folder:

□ Login as console/admin session

□ Server is TS Farm

⊞ Show advanced Windows options

☑ Automatically log in

● Use SSL VPN account credentials

□ Use Login Domain for SSO

○ Use custom credentials

□ Display Bookmark to Mobile Connect clients

**Tips/Help**

**Which version of RDP should I use?**

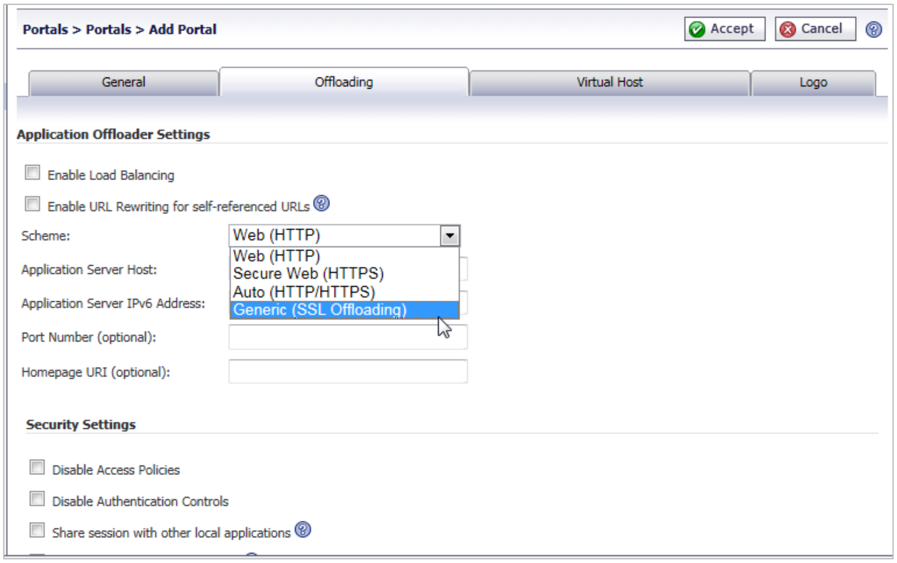
If you are using Internet Explorer on Windows, you can use the ActiveX version. For all other browsers and operating systems, you should use the Java version.

**How can I find my MAC address?**

On the Windows computer that will act as the RDP server, open a command window and run "ipconfig /all", then look for "physical address".

### Application Offloading Enhancement

Generic (SSL Offloading) has been added to the Scheme drop-down list shown on the Offloading tab of the Portals > Portals > Offload Web Application page for SRA 1200 and 1600 appliances. This option allows users to configure generic SSL offloading support on the SRA 1200 and 1600 appliances, which is already supported on other SRA appliances.



**Application Offloader Settings**

□ Enable Load Balancing

□ Enable URL Rewriting for self-referenced URLs

Scheme: Web (HTTP)

- Web (HTTP)
- Secure Web (HTTPS)
- Auto (HTTP/HTTPS)
- Generic (SSL Offloading)

Application Server Host:

Application Server IPv6 Address:

Port Number (optional):

Homepage URI (optional):

**Security Settings**

□ Disable Access Policies

□ Disable Authentication Controls

□ Share session with other local applications

## Known Issues

This section contains a list of known issues in the SRA 7.5.0.0 release.

### *Bookmarks*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| Bookmark disconnects after about two minutes. | Occurs on some Windows 8 client machines with ActiveX or Java bookmark.<br>**Workaround**: Use NetExtender and then run your RDP client of choice or utilize the Tunneled bookmark option available with SRA 7.5. | 127258 |

### *Licensing*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| A Spike License can be automatically activated by exceeding the normally allowed number of connections even if Spike Licensing is not a currently licensed service on the SRA appliance. | Occurs when the “Automatically activate Spike License” option is left enabled on an appliance that was previously licensed for Spike Licensing, but then had the license removed. | 140468 |

### *NetExtender*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| NetExtender fails to install and gives the error message, "Failed to validate the server, the server may be running on an old or incompatible firmware!" | Occurs when logging into the user portal from a machine running Windows Server 2003 R2/SP2 and clicking on the button to install NetExtender.<br>**Workaround**: Use the .exe or .MSI file available on MySonicWALL to install NetExtender. | 140601 |
| NetExtender fails to reconnect after upgrading and displays the error message, “Verifying user…” | Occurs when the 7.0 NetExtender client is used to connect to an SRA appliance running 7.5.0.0, and certificate authentication is enabled. NetExtender automatically upgrades to the 7.5 client, but does not reconnect to the appliance. | 139757 |
| Voice calls, video calls, and desktop sharing from/to a LAN cannot be established using Lync. | Occurs when using NetExtender from Mac OS X when in a SSL VPN tunnel. | 125695 |

### *Reverse Proxy*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| Clicking on a VNC–HTML5 bookmark launches a blank window. | Occurs when a user connects to the portal on the SRA appliance using PAT (Port Address Translation), then creates a VNC–HTML5 bookmark and clicks on it to launch the application. | 138906 |

## Resolved Issues

The following issues are resolved in the SRA 7.5.0.0 release:

### *Citrix*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| Citrix 6.5 applications do not launch correctly and Java errors might occur. | Occurs when launching a Citrix 6.5 application via a bookmark on the SRA user portal. | 126749 |

### *EPC*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| EPC fails when logging in. | Occurs when Avast Free AntiVirus 8.0 or 9.0 software is installed and added to the local group or user profile.<br>**Workaround**: Use Avast Free AntiVirus 7.0. | 137110 |
| Recurring EPC does not warn or log out user. | Occurs when using recurring EPC with a portal.<br>**Workaround**: Use the NetExtender client. | 125536 |
| Users from a client machine that does not meet EPC requirements can login and access an offloaded application. | Occurs when using EPC with an offloaded portal. | 124262 |

### *Logs*

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| With log automation configured on the SRA appliance to email the log when full or on a daily basis, an incorrect event log file without all log entries is emailed. | Occurs after a log rotation when the older rotated file is emailed instead of the most recent rotated file. | 135079 |
| A Viewpoint server does not display the IP address information for backend resources that a NetExtender user accesses. | Occurs when the SRA appliance is configured for local user authentication and is connected to a Viewpoint server for reporting purposes, and a user connects using NetExtender and accesses a backend resource.<br>Resolved by introducing a NetExtender > Log page with the resource access details. | 103899 |

### NetExtender

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| NetExtender cannot be installed from Virtual Office and the Java console log contains the *java(16802) deny process-execu /user/sbin/netExtender* message. | Occurs when using Mac OS X 10.9 because Java applets are installed by default in a sandbox environment.<br>**Workaround:** Select the **Manually download NetExtender** link from the installer dialog or open Safari Preferences > Security > Manage Website Plug-ins and select **Run in Unsafe mode**. | 138302 |
| A user without privileged access can gain root access on Linux or Mac OS. | Occurs when the user appends exploit code to the end of the script that keeps track of NetExtender routes to be cleaned up after NetExtender exits. | 136159 |
| There is no way to push a login script from the SRA appliance out to connecting users based on user, group, or global control policies. Such scripts must be installed individually on each client machine. | Occurs when login scripts or post-connection scripts are required by the SRA administrator to perform tasks on client machines right after the users connect via NetExtender. | 131956 |
| There is no way configure the SRA appliance to provision NetExtender connections so that all user Internet traffic is routed through a designated proxy server. | Occurs when the SRA administrator wants to manage user access to the Internet via settings on the proxy server.<br>Resolved by adding Internal Proxy Settings fields to the SRA appliance NetExtender configuration options for use with Internet Explorer on Windows machines. After NetExtender connects to the SRA appliance, the internal proxy settings are pushed to the client and used as proxy settings for the NetExtender virtual adapter. | 128466 |

### Portals

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| Not all SRA appliances support Generic SSL Offloading. | Occurs when using an SRA 1200 or SRA 1600 and viewing the options in the Scheme drop-down list on the Offloading tab after clicking Offload Web Application on the Portals > Portals page. The “Generic (SSL Offloading)” option is now available on these platforms when running SRA 7.5.0.0. | 136129 |
| It should be possible to utilize userPrincipalName as a login attribute to Virtual Office. | Occurs when the sAMAaccountName, CN, and uid attributes are not adequate for the administrator’s requirements.<br>SRA 7.5.0.0 supports the userPrincipalName attribute for Active Directory type LDAP servers. | 133634 |
| SRA can only work with Citrix CloudGateway Express / Storefront by configuring tunnel access to it via NetExtender. | Occurs when Storefront is deployed on Citrix XenApp 6.5 and the SRA administrator wants to set up a bookmark to it or configure application offloading for it. | 125474 |

### System

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| Scheduled reboot does not occur. | Occurs when reboot is scheduled using the diag page. | 136860 |
| Browser access to the appliance stops working and “Reset adapter” messages are displayed on the console. Browser access is restored by rebooting the appliance. | Occurs intermittently on SRA 4600 and SRA 1600 appliances. | 124107 |
| The SRA appliance sometimes loses network connectivity and must be restarted from the console. After the reboot command is entered in the console, driver error messages are displayed, “e1000_clean_tx_irq: Detected Tx Unit Hang”. | Occurs intermittently on SRA 4200 and SRA 1200 appliances. | 89329 |

### Users

| Symptom | Condition / Workaround | Issue |
|---|---|---|
| It should be possible to configure user login schedules on the SRA appliance. | Occurs when the SRA administrator wants to restrict access to certain times or days. | 41620 |

## Upgrading SRA Image Procedures

The following procedures are for upgrading an existing SRA firmware image or Virtual Appliance software image to a newer version:

***Note:*** *For the SRA 7.5.0.0 release only, a Virtual Appliance cannot be upgraded to SRA 7.5 because of Operating System changes in the Virtual Appliance software. Instead, install SRA 7.5 as explained in Moving a Virtual Appliance to 7.5 on page 30.*

### *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 you 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_7.5.0.0_7.5.0_p_15sv_630652.sig**

   For the Dell SonicWALL Virtual Appliance, this is a file such as:
   **sw_sslvpnsra-vm_eng_7.5.0.0_7.5.0_p_15sv_630652.ova**
   **sw_sslvpnsra-vm_eng_7.5.0.0_7.5.0_p_15sv_630652.sig**

   ***Note****: For SRA Virtual Appliances, image files for new deployments have a* ***.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.

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. 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

***Note**: 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 – New!** . 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 preference, click the boot icon for the following entry:

     **Uploaded Firmware – New!**
   - To reboot the image with factory default settings, click the boot icon for the following entry:

     **Uploaded Firmware with Factory Defaults – New!**

   ***Note**: Be sure to save a backup of your current configuration settings to your local machine 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 **OK**, 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.*

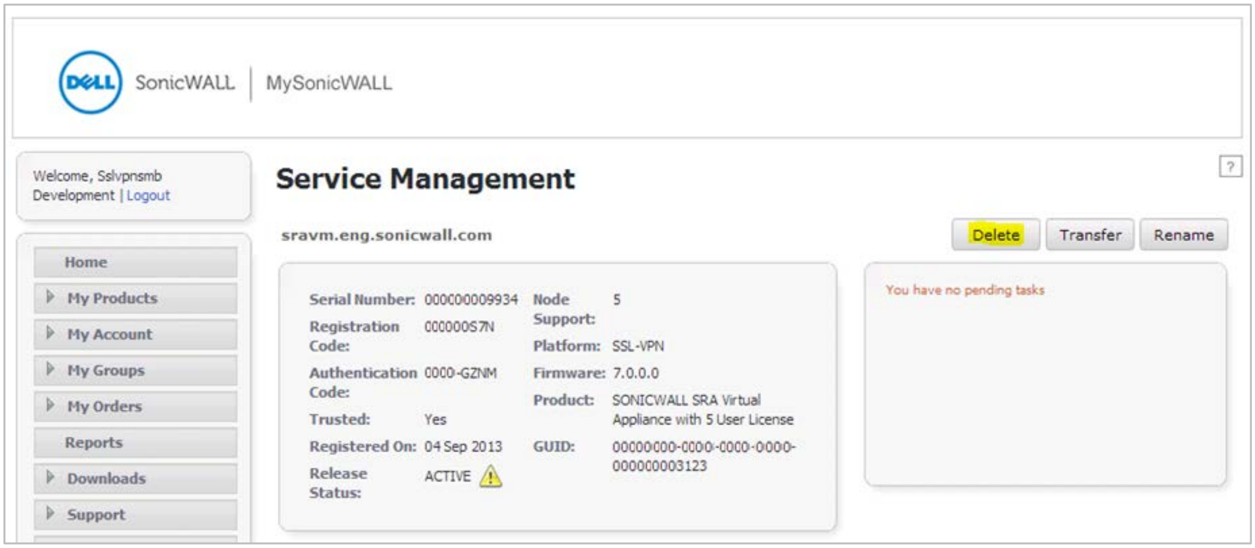
   The **Test** light starts blinking when the Dell SonicWALL security appliance has rebooted into SafeMode.
3. Connect to the management interface by pointing the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.
4. Try rebooting the Dell SonicWALL 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 7.5.0.0*

For the SRA 7.5.0.0 release only, a Virtual Appliance cannot be upgraded to SRA 7.5 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 28.
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 7.5.0.0 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.



Service Management

sravm.eng.sonicwall.com

Serial Number: 000000009934
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

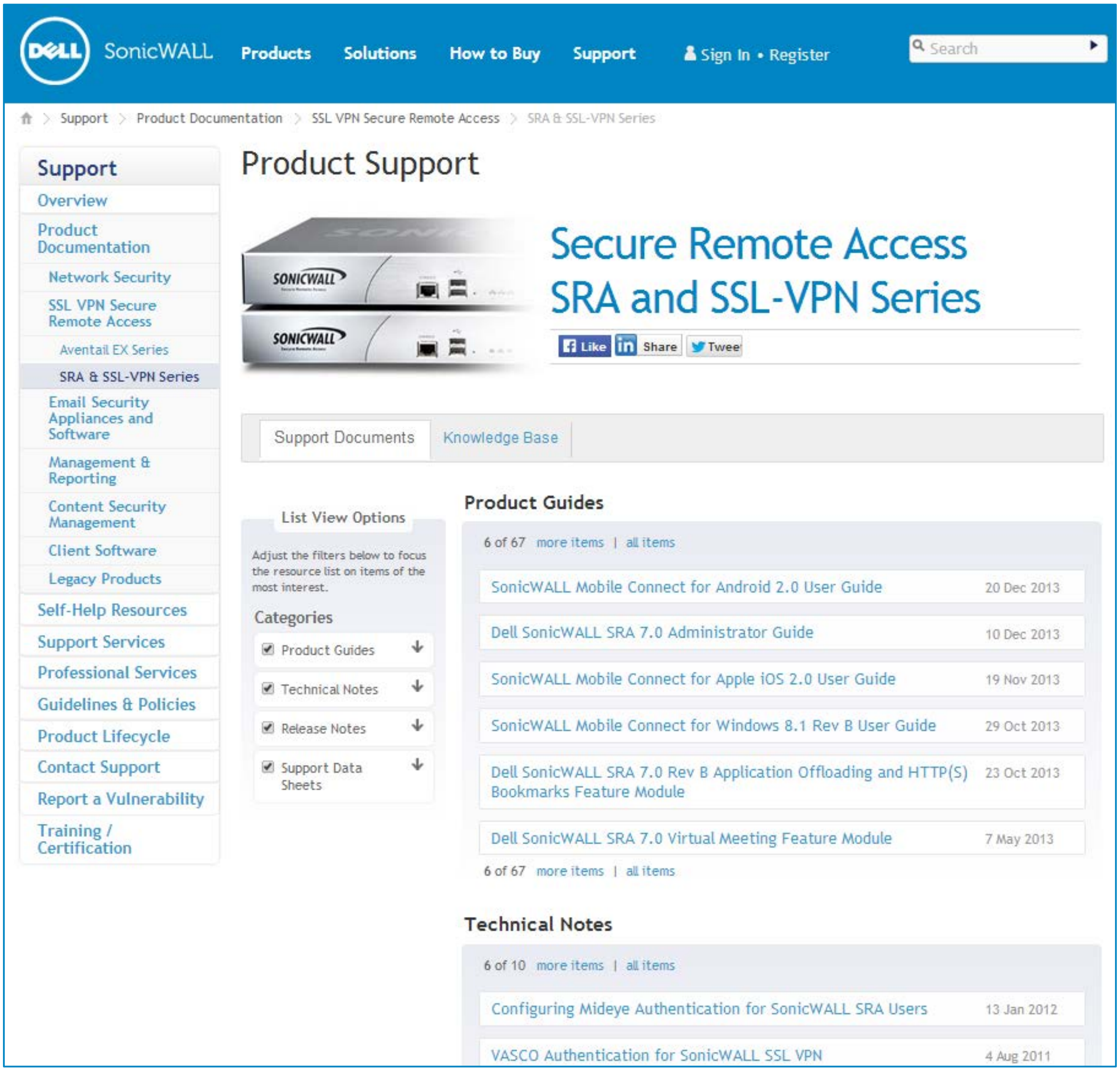
8. Register the new virtual appliance from the System > Licenses page. Enter the serial number and authentication code noted in step #2 above.

   This transfers all the licensed services from the old virtual appliance to the new virtual appliance.

## Related Technical Documentation

Related technical documentation is available on the Dell SonicWALL Online Library at:

http://www.sonicwall.com/us/Support.html



Product Support

Secure Remote Access SRA and SSL-VPN Series

Adjust the filters below to focus the resource list on items of the most interest.

Product Guides

| | |
|---|---|
| SonicWALL Mobile Connect for Android 2.0 User Guide | 20 Dec 2013 |
| Dell SonicWALL SRA 7.0 Administrator Guide | 10 Dec 2013 |
| SonicWALL Mobile Connect for Apple iOS 2.0 User Guide | 19 Nov 2013 |
| SonicWALL Mobile Connect for Windows 8.1 Rev B User Guide | 29 Oct 2013 |
| Dell SonicWALL SRA 7.0 Rev B Application Offloading and HTTP(S) Bookmarks Feature Module | 23 Oct 2013 |
| Dell SonicWALL SRA 7.0 Virtual Meeting Feature Module | 7 May 2013 |

Technical Notes

| | |
|---|---|
| Configuring Mideye Authentication for SonicWALL SRA Users | 13 Jan 2012 |
| VASCO Authentication for SonicWALL SSL VPN | 4 Aug 2011 |

Information about Dell SonicWALL SRA is found in the many reference guides available on the Web site, including:

- *Dell SonicWALL SRA Administrator’s Guide*
- *Dell SonicWALL SRA User’s Guide*
- *Dell SonicWALL SRA NetExtender Feature Module*
- *Dell SonicWALL SRA Citrix Access Feature Module*
- *Dell SonicWALL SRA Web Application Firewall Feature Module*
- *Dell SonicWALL SRA Application Offloading and HTTP(S) Bookmarks Feature Module*

Last updated: 1/29/2014