SonicWall™ Secure Mobile Access 8.6.0.1

Release Notes

April 2017

These release notes provide information about the SonicWall Secure Mobile Access (SMA) 8.6.0.1 release.

About Secure Mobile Access 8.6.0.1

Secure Mobile Access (SMA) 8.6.0.1 is a feature release for SonicWall SMA 400, SMA 200, SRA 4600, SRA 1600, and SMA 500v.

Supported platforms

The SMA 8.6.0.1 release is supported on the following SonicWall platforms:

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

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

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

New Features

This section describes the new features in the SMA 8.6.0.1 release.

- Product/documentation rebranded
- HTML5 RDP enhancements
- Remote Desktop Web Access support
- SONAR product analytics
- Miscellaneous enhancements

HTML5 RDP enhancements

The HTML5 RDP feature continues to improve with additional functionality and improved usability.

Included improvements:

- Printer redirection.
- Time-Zone redirection
- Load balance information
- RDP options import

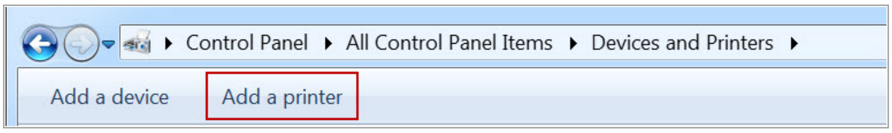
Printer redirection

HTML5 RDP can support a specific Printer Driver Redirection – “MS Publisher Imagesetter.” If the Remote Desktop Session Host server has the driver installed. HTML5 RDP can redirect the printer to the client side. The user can select the Redirection Printer to print this file to a PDF. After the PDF is created, a file pop-up viewer appears. You can “Print Preview” the PDF file or print the file directly.

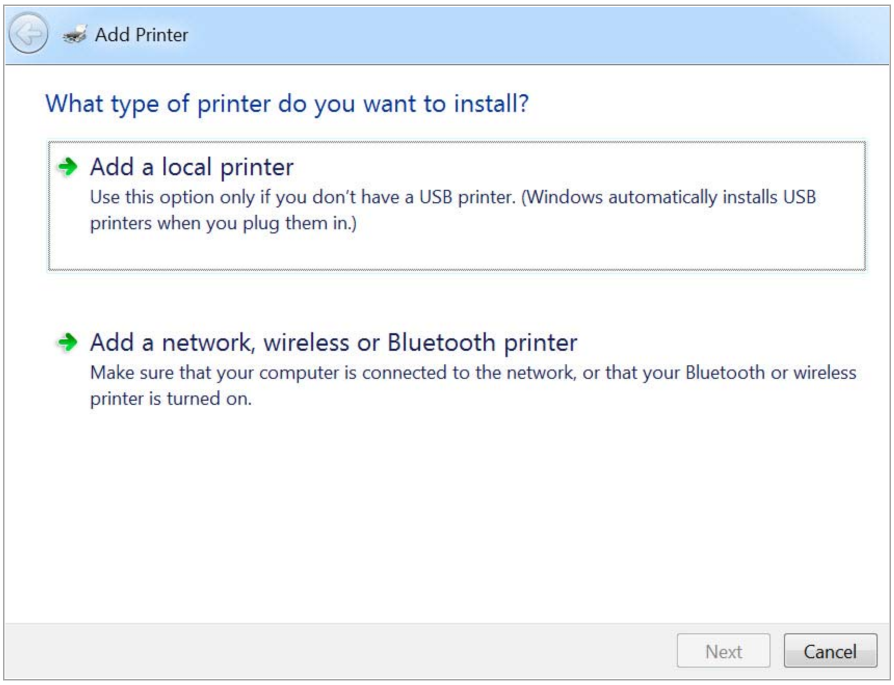
To install the MS Publisher Imagesetter on Windows 7:

1 Go to **Windows Control Panel** and click **Devices and Printers**.

2 Click “Add a printer.”



3 Select “Add a local printer.”



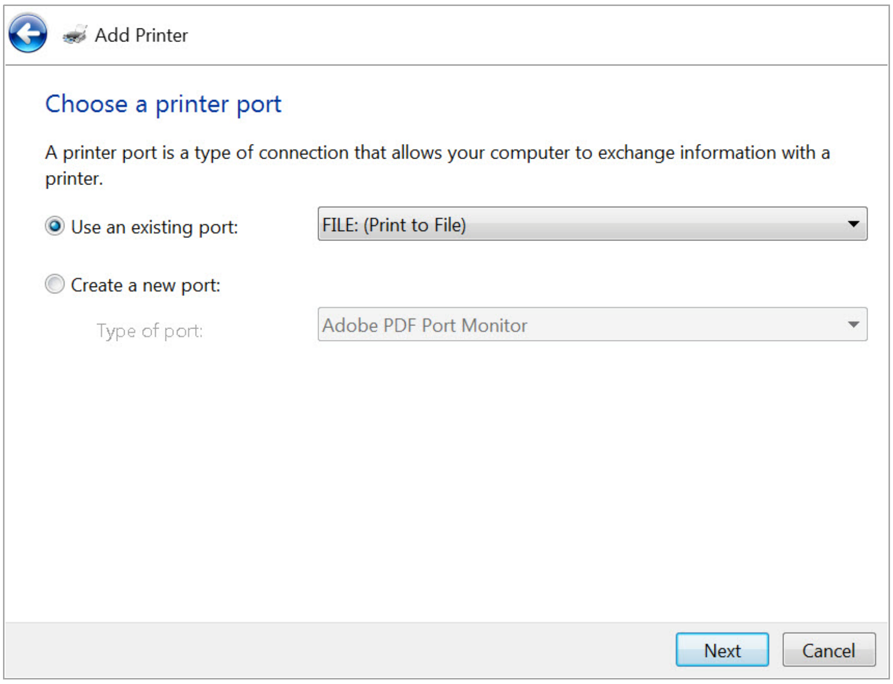
Add Printer

What type of printer do you want to install?

➔ Add a local printer
Use this option only if you don’t have a USB printer. (Windows automatically installs USB printers when you plug them in.)

➔ Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4 Select “Use an existing port” and select “FILE: (Print to File)” in the drop-down box.



Add Printer

Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

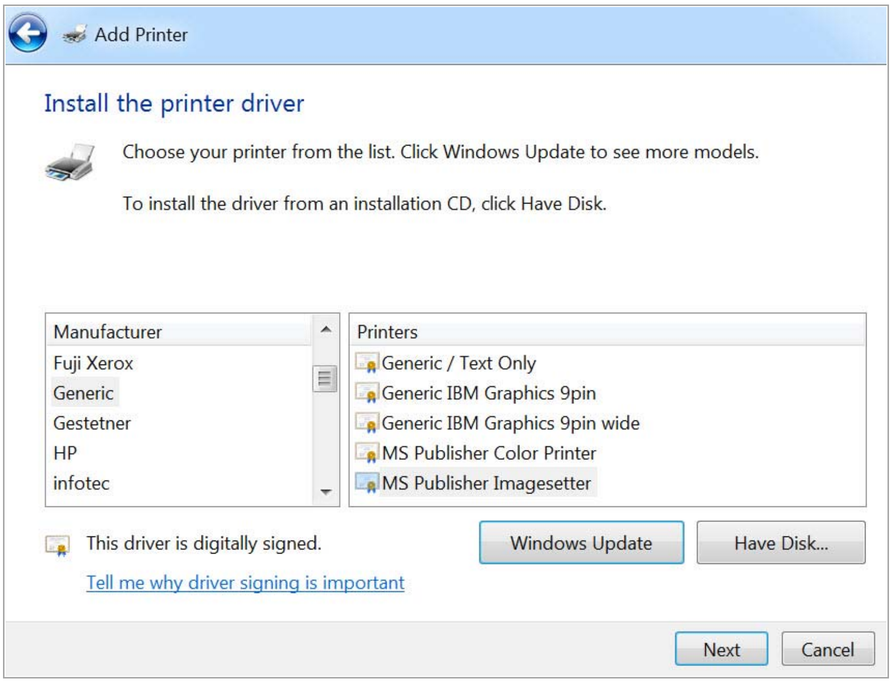
● Use an existing port: FILE: (Print to File)

○ Create a new port:

Type of port: Adobe PDF Port Monitor

5 Click **Next**.

6 Select **Generic** from the **Manufacturer** list. Then select **MS Publisher Imagesetter** from the **Printers** list.



Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

This driver is digitally signed.

Tell me why driver signing is important

7 Click **Next**.

8 Select "**Use the driver that is currently installed**."

9 Click **Next**.

10 Use the default settings for the Printer name, "**MS Publisher Imagesetter**."

11 Click **Next**.

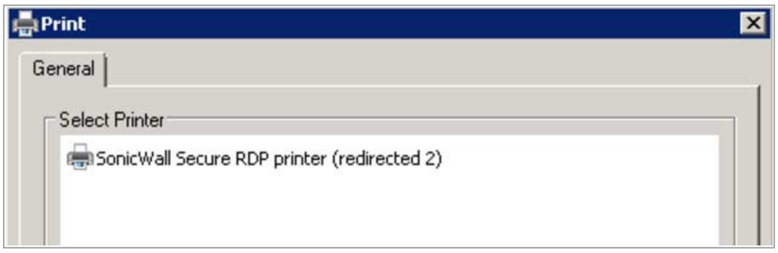
12 Select the option that best suits your sharing criteria.

13 Click **Next**.

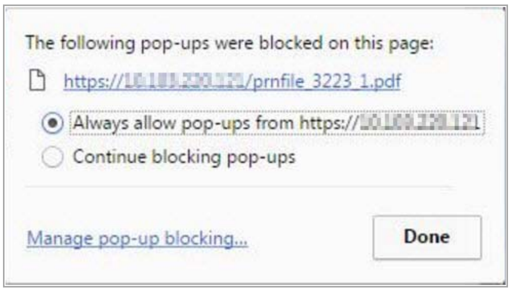
14 Click **Finish**. You should find your new printer in the "Printers and Faxes" area.

Enable the Redirection Printers

1 Enable the Redirection Printers in the "Show Advanced Windows Options" of the bookmark. After the Redirection Printer is enabled, you can find the "SonicWall Secure RDP Printer" in the remote server's printer list.



2 Select the printer to print the file. The browser might attempt to block the pop-up window. Select “Always allow pop-ups from https://...” (the server address).



The following pop-ups were blocked on this page:

https://[redacted]/prnfile_3223_1.pdf

● Always allow pop-ups from https://[redacted]

○ Continue blocking pop-ups

3 You can now preview the file and print it on the local printer.

Time-zone redirection

HTML5 RDP can also redirect the local time-zone to the remote server. The remote server should enable this feature.

The following steps show how to enable time-zone redirection in Windows 2008 R2:

1 Open **Local Group Policy Editor** or **Group Policy Management**.

2 Use the following path:

Computer Configuration > (Policies) > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection > Allow time zone redirection.

3 Double click the printer name and select **Enabled**.

4 Click **OK**.

After enable the setting on the remote server, you can see the local time-zone is redirected to the remote server.

Time zone redirection is possible only when connecting to at least a Windows Server 2003 terminal server with a client that is using RDP 5.1 or later.

Load Balance Information

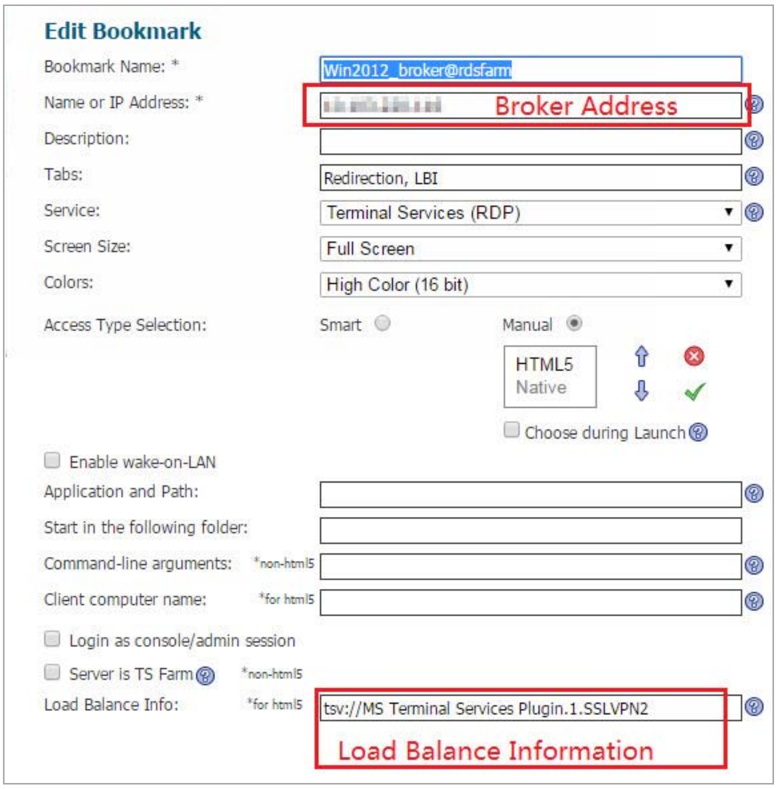
In Windows 2012, there is a new way to do the redirection (load balance). The RDP client can connect to the broker server directly, and then the broker server returns the redirection information to the client. The RDP client can connect to the RDP Host in the “Collection.”

When you access the Windows 2012 RD Web, download the RDP file by clicking the item on the page. The RDP file contains a line with the following string:

```
“loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.<CollectionName>”
```

The <CollectionName> is the collection name in the user’s farm. This line is the “Load Balance Information.” The broker server needs this information to do the load balancing (redirection).

The following screen shows how to use the “Load Balance.”



Edit Bookmark

Bookmark Name: *	Win2012_broker@rdsfarm
Name or IP Address: *	[redacted]
Description:	
Tabs:	Redirection, LBI
Service:	Terminal Services (RDP)
Screen Size:	Full Screen
Colors:	High Color (16 bit)
Access Type Selection:	Smart ○ Manual ●
	HTML5 Native
	□ Choose during Launch
□ Enable wake-on-LAN	
Application and Path:	
Start in the following folder:	
Command-line arguments: *non-html5	
Client computer name: *for html5	
□ Login as console/admin session	
□ Server is TS Farm *non-html5	
Load Balance Info: *for html5	tsv://MS Terminal Services Plugin.1.SSLVPN2

Importing RDP Options

There are many RDP options and the HTML5/Native RDP just supports some of them. Sometimes the user cannot know all options of RDP. So we add a new feature to help user to import the options in the RDP file into the RDP bookmark.

The following steps show how to import RDP file options into the bookmark:

1 Start by creating a new bookmark or opening an existing bookmark.

2 Click **Import RDP Options**.

3 Open the RDP file with a text editor (such as Notepad) and select the entire file content.

4 Copy the content and paste the text into the text field in **Import RDP Options**.

5 Click **OK**. The feature selects the support options to import into the bookmark.

The following table lists the RDP options and the RDP file options.

Bookmark field	RDP option
Name or IP Address	full address:s:<value>
Screen Size	desktopheight:i:<value> desktopwidth:i:<value>
Colors	session bpp:i:<value>
Load Balance Info	loadbalanceinfo:s:<value>
Desktop Background	disable wallpaper:i:<value>
Auto-Reconnection	autoreconnection enabled:i:<value>
Menu/Window Animation	disable menu anims:i:<value>
Visual Styles	disable themes:i:<value>
Show Window contents while dragging/resizing	disable full window drag:i:<value>

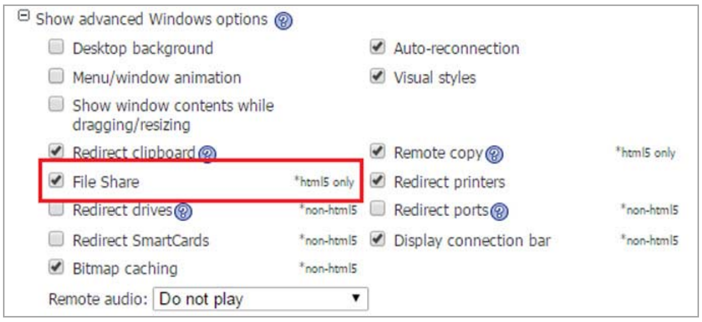
Bookmark field	RDP option
Redirect clipboard & Remote Copy	redirectclipboard:i:<value>
Redirect printers	redirectprinters:i:<value>
Redirect drives	redirectdrives:i:<value>
Redirect ports	redirectcomports:i:<value>
Redirect SmartCards	redirectsmartcards:i:<value>
Display connection bar	displayconnectionbar:i:<value>
Bitmap caching	bitmapcachepersistenable:i:<value>
Remote audio	audiomode:i:<value>
Font smoothing	allow font smoothing:i:<value>
Span monitors	span monitors:i:<value>
Dual monitors	use multimon:i:<value>
Desktop composition	allow desktop composition:i:<value>
Remote Application	remoteapplicationmode:i:<value>
Choose your connection speed to optimize performance	connection type:i:<value>

File transferring

HTML5 file sharing is embedded in HTML5 RDP. You can enable this feature and access the shared folder of the Remote Server from the HTML5 RDP page.

The following steps show how to enable and use the file sharing feature:

1 Edit the HTML5 RDP bookmark page to enable the feature.

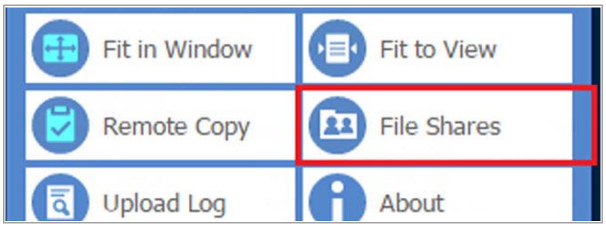


⊟ Show advanced Windows options

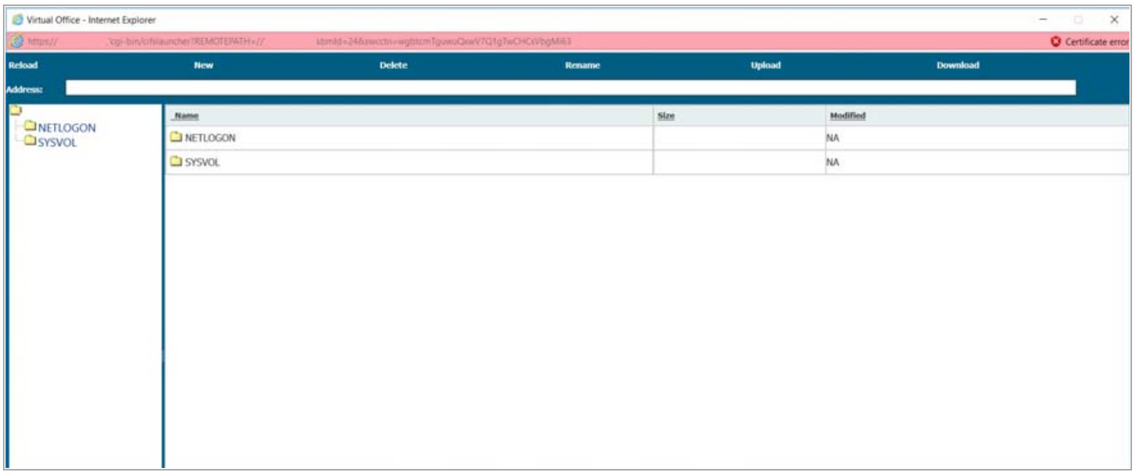
- ☐ Desktop background
- ☐ Menu/window animation
- ☐ Show window contents while dragging/resizing
- ☑ Redirect clipboard
- ☑ File Share *html5 only
- ☐ Redirect drives *non-html5
- ☐ Redirect SmartCards *non-html5
- ☑ Bitmap caching *non-html5
- ☑ Auto-reconnection
- ☑ Visual styles
- ☑ Remote copy *html5 only
- ☑ Redirect printers
- ☐ Redirect ports *non-html5
- ☑ Display connection bar *non-html5

Remote audio: Do not play ▾

2 You will see a new button for the feature on the HTML5 RDP menu after clicking the Shield icon.



3 Click **Files Shares**, the File Share window opens. You can manipulate the folders and files in the window.



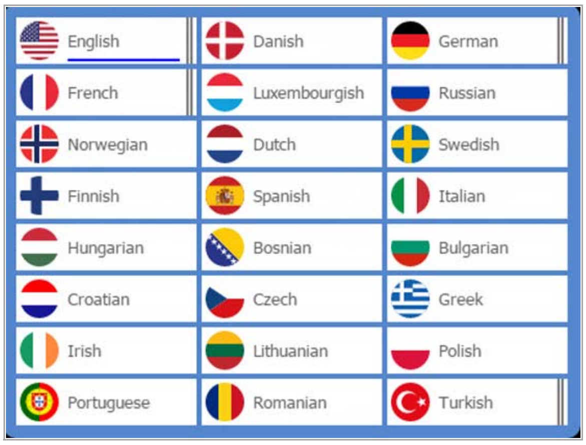
Name	Size	Modified
NETLOGON		NA
SYSVOL		NA

More European keyboard support

SMA 8.6.0.1 provides additional European keyboard support. The available keyboards are listed as follows:

Countries	Keyboards	Languages
Bosnia	Bosnian (Cyrillic)	Bosnian (Cyrillic, Bosnia and Herzegovina)
Bulgaria	Bulgarian	Bulgarian (Bulgaria)
Croatia	Croatian	Croatian (Croatia)
Czech Republic	Czech	Czech (Czech Republic)
Greece	Greek	Greek (Greece)
Hungary	Hungarian	Hungarian (Hungary)
Ireland	Irish	Irish (Ireland)
Lithuania	Lithuanian	Lithuanian (Lithuania)
Poland	Polish(214)	Polish (Poland)
Portugal	Portuguese	Portuguese (Portugal)
Romania	Romanian (Legacy)	Romanian (Romania)
Turkey	Turkish F	Turkish (Turkey)
Turkey	Turkish Q	Turkish (Turkey)
English	United States-International	English (United States)

The menu appears as follows:



English	Danish	German
French	Luxembourgish	Russian
Norwegian	Dutch	Swedish
Finnish	Spanish	Italian
Hungarian	Bosnian	Bulgarian
Croatian	Czech	Greek
Irish	Lithuanian	Polish
Portuguese	Romanian	Turkish

Keep the keyboard language settings consistent between these three areas:

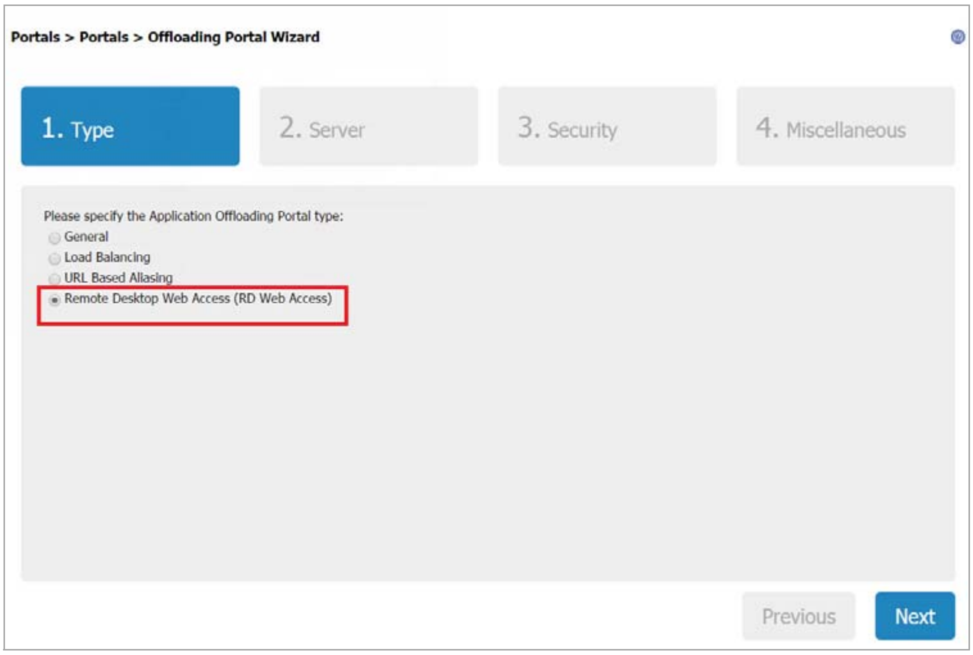
1. Local client machine
2. HTML5 settings
3. Remote RDP server machine

Remote Desktop Web Access support

The Remote Desktop (RD) Web Access page has been rewritten, and now uses the SMA Agent to proxy the RDP connection to the private network to make the resource list on the RD Web site function more efficiently. Another advantage is that the rewritten RD Web Access site now works for all browsers (Chrome, Firefox, IE…).

Configuring the Application Offloading Portal

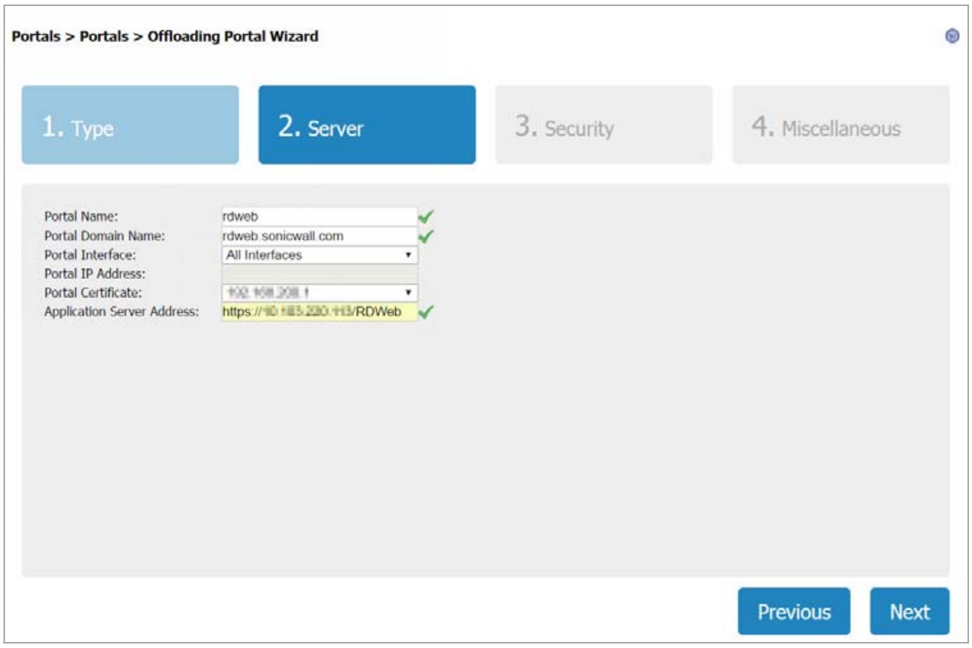
A new RD Web Access portal has been created that mimics a standard offloading portal. Select R**emote Desktop Web Access (RD Web Access)** when selecting the portal type in the wizard steps.



Please specify the Application Offloading Portal type:

○ General
○ Load Balancing
○ URL Based Aliasing
● Remote Desktop Web Access (RD Web Access)

Complete the Server page similar to as follows:

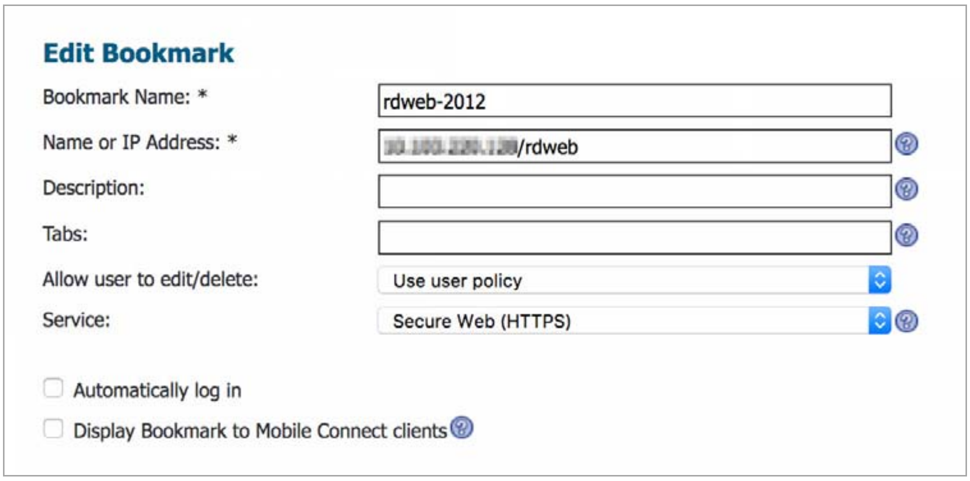


Portals > Portals > Offloading Portal Wizard

Portal Name:	rdweb ✓
Portal Domain Name:	rdweb.sonicwall.com ✓
Portal Interface:	All Interfaces
Portal IP Address:	
Portal Certificate:	[redacted]
Application Server Address:	https://[redacted]/RDWeb ✓

Configuring the HTTPS bookmarks

Configure the HTTPS bookmark as follows:



Edit Bookmark

Bookmark Name: *	rdweb-2012
Name or IP Address: *	[redacted]/rdweb
Description:	
Tabs:	
Allow user to edit/delete:	Use user policy
Service:	Secure Web (HTTPS)

□ Automatically log in

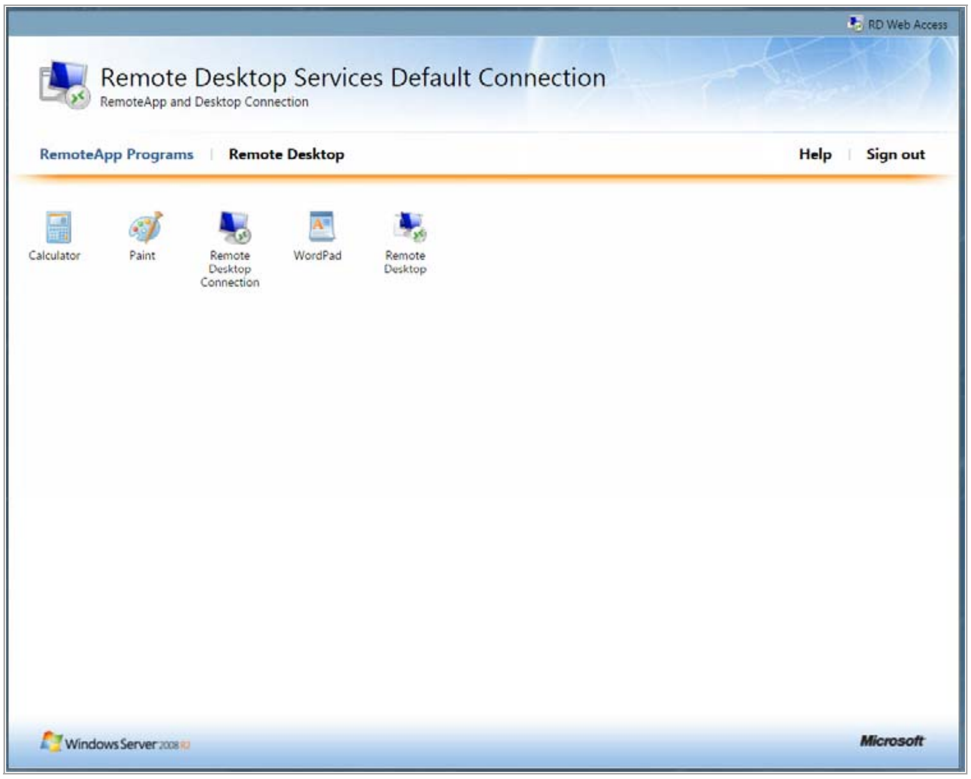
□ Display Bookmark to Mobile Connect clients

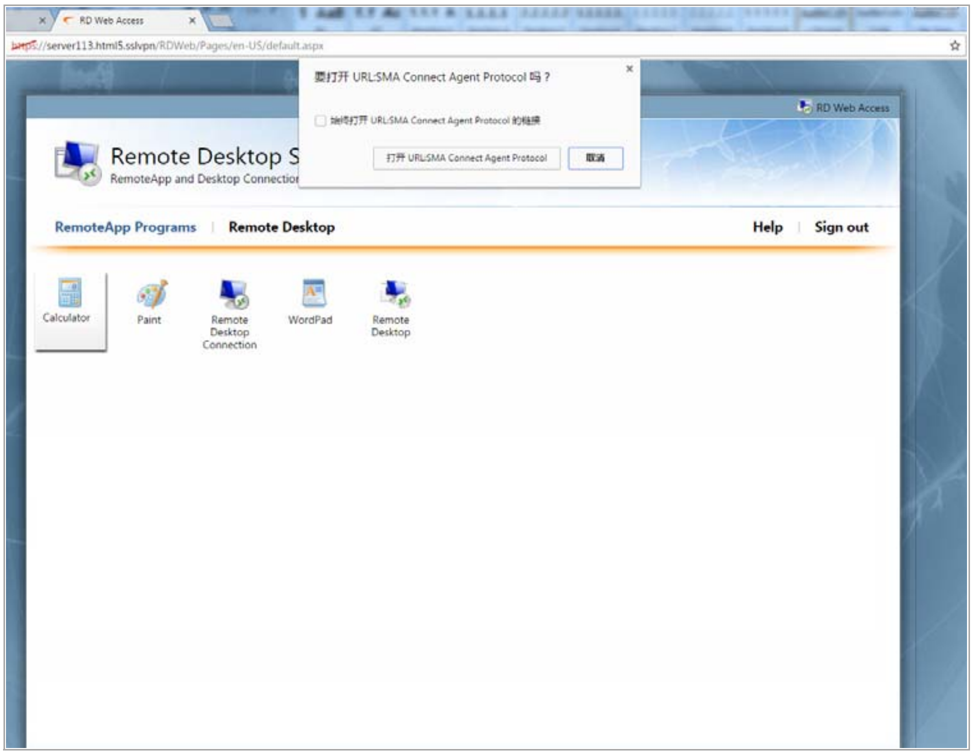
Access Application Offloading Portal/HTTPS Bookmark

If the SMA Agent is not installed, download and install it from the following URL:

https://yoursslvpnappliance/SMAConnectAgent.msi

After the SMA Agent is installed, you can then transparently access the RemoteApp Programs and TS session host the same as before, as shown in the following images:

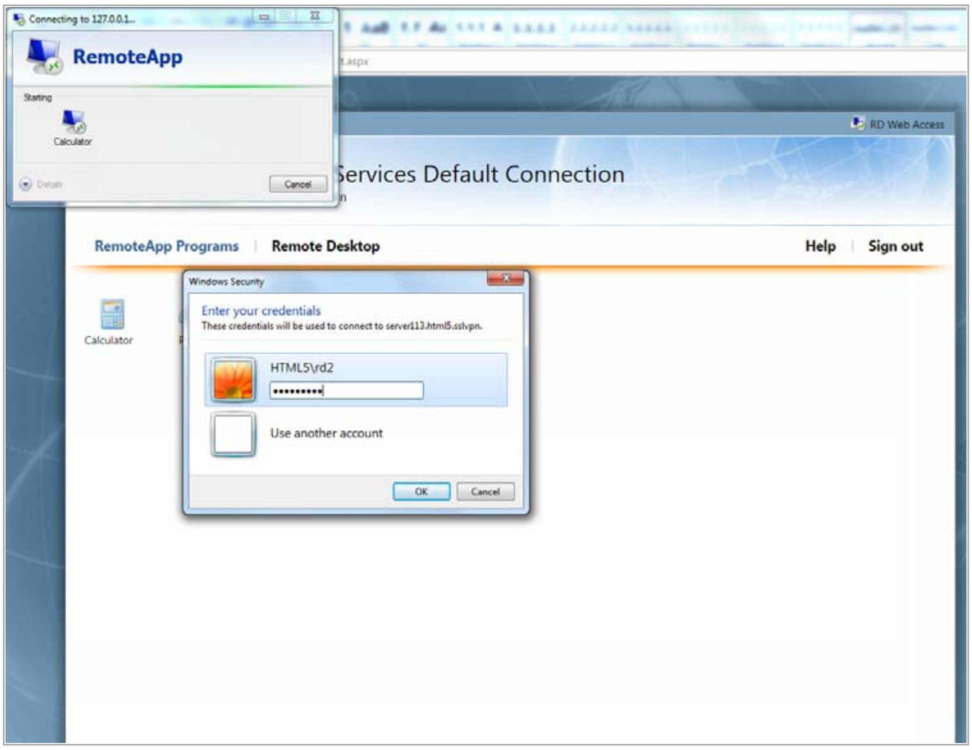




要打开 URL:SMA Connect Agent Protocol 吗？

□ 始终打开 URL:SMA Connect Agent Protocol 的链接

打开 URL:SMA Connect Agent Protocol | 取消

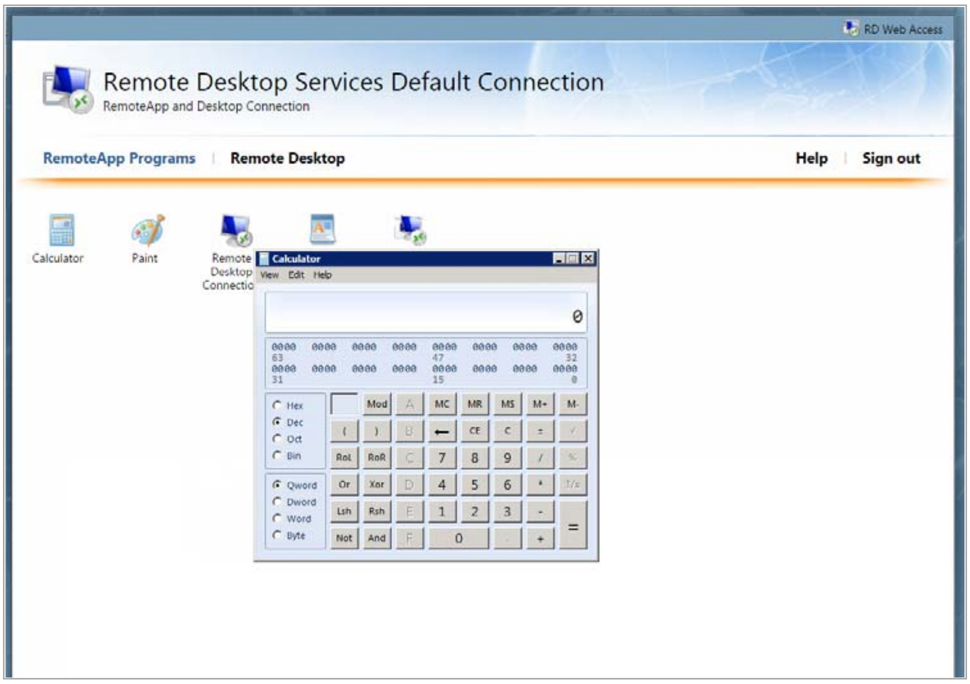


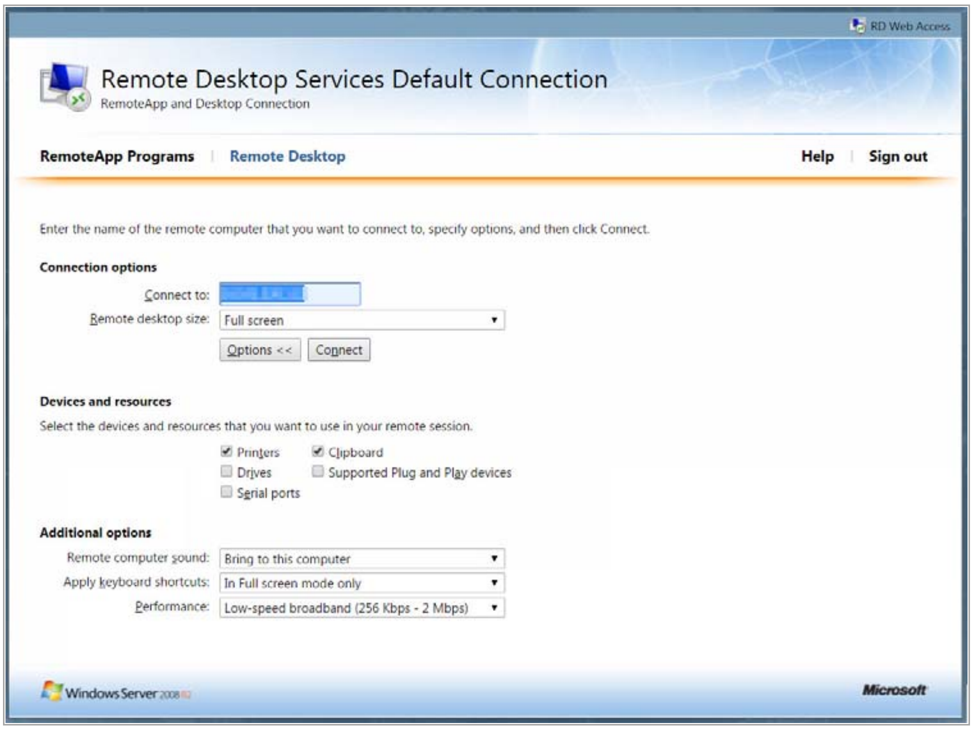
Enter your credentials

These credentials will be used to connect to server113.html5.sslvpn.

HTML5\rd2

•••••••••




RD Web Access
Remote Desktop Services Default Connection
RemoteApp and Desktop Connection
RemoteApp Programs
Remote Desktop
Help
Sign out

Enter the name of the remote computer that you want to connect to, specify options, and then click Connect.

Connection options

Connect to: [illegible]

Remote desktop size: Full screen

Devices and resources

Select the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard
☐ Drives ☐ Supported Plug and Play devices
☐ Serial ports

Additional options

Remote computer sound: Bring to this computer

Apply keyboard shortcuts: In Full screen mode only

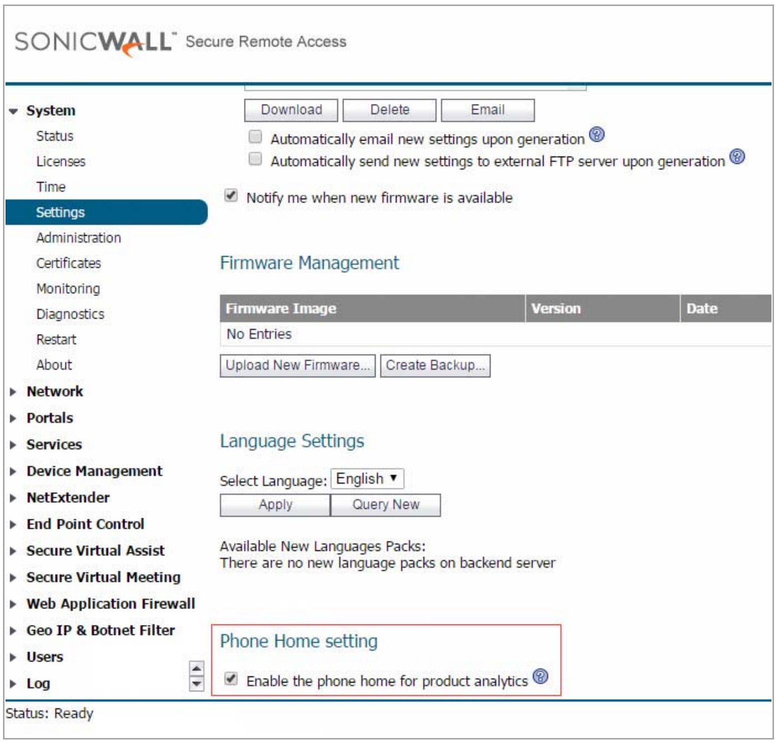
Performance: Low-speed broadband (256 Kbps - 2 Mbps)

SONAR product analytics

Enhanced Product Analytics, also known as “phone home,” uses the MSW backend server to collect phone home data from your appliance. The collected data is divided into two parts. The first part is the static license and configuration data that indicates configured numbers. The second part is the run-time data that indicates usage numbers. Based on this data and subsequent analytics, this data can be accurately tracked and improved or deprecated effectively.

Enabling or disabling SONAR product analytics

You can enable or disable the Phone Home settings by accessing them on the **System > Settings** page and selecting or deselecting the **Enable the phone home for product analytics** option.



☐ Automatically email new settings upon generation

☐ Automatically send new settings to external FTP server upon generation

☑ Notify me when new firmware is available

Firmware Management

Firmware Image	Version	Date
No Entries		

Language Settings

Select Language: English

Available New Languages Packs:
There are no new language packs on backend server

Phone Home setting

☑ Enable the phone home for product analytics

Status: Ready

Miscellaneous enhancements

Along with the previously mentioned additional features, SMA 8.6.0.1 also includes a list of miscellaneous enhancements including:

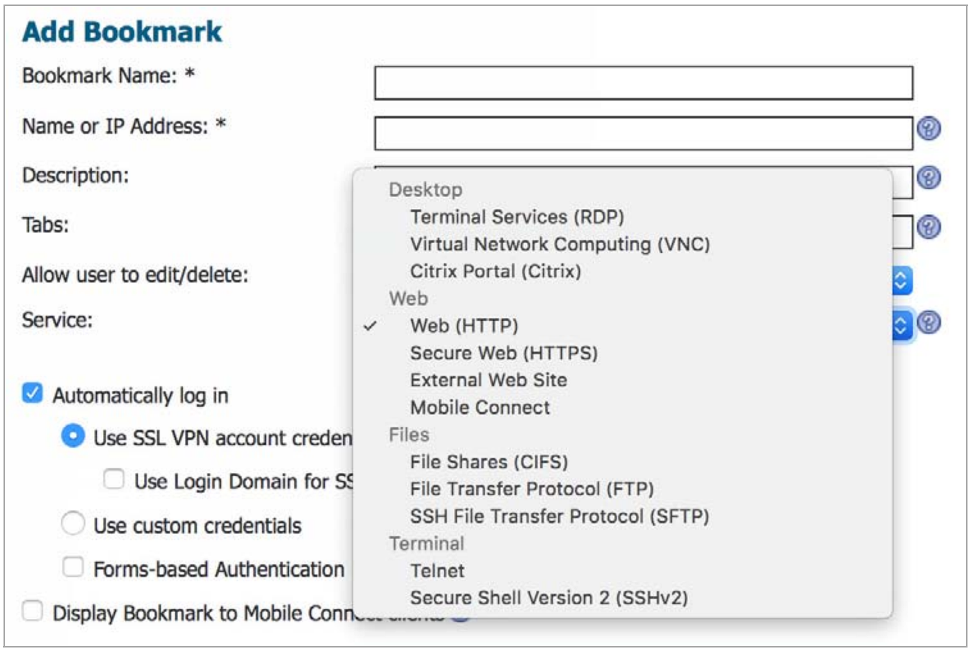
- Deprecating Java bookmarks
- Moving clients from the firmware to the backend server
- Deprecating the VirtualAssist and VirtualMeeting web interfaces

Deprecating Java bookmarks

Alternative solutions (HTML5 bookmarks) have been developed to replace the notoriously insecure Java bookmarks. In the SMA 8.6.0.1 release, the Java bookmarks have been deprecated and disabled by default. If a Java bookmark is still required, contact Support for the steps necessary to enable the bookmark.

All bookmark options are adjusted accordingly, and Java-related options have been removed.

When adding a new bookmark, the **Secure Shell Version 1 (SSHv1)** service type has been removed. Existing SSHv1 bookmarks still exists within the system, but are hidden on the Portal page. If Java bookmarks have been enabled manually, they will be visible.



Add Bookmark

Bookmark Name: *

Name or IP Address: *

Description:

Tabs:

Allow user to edit/delete:

Service:

☑ Automatically log in

● Use SSL VPN account creden

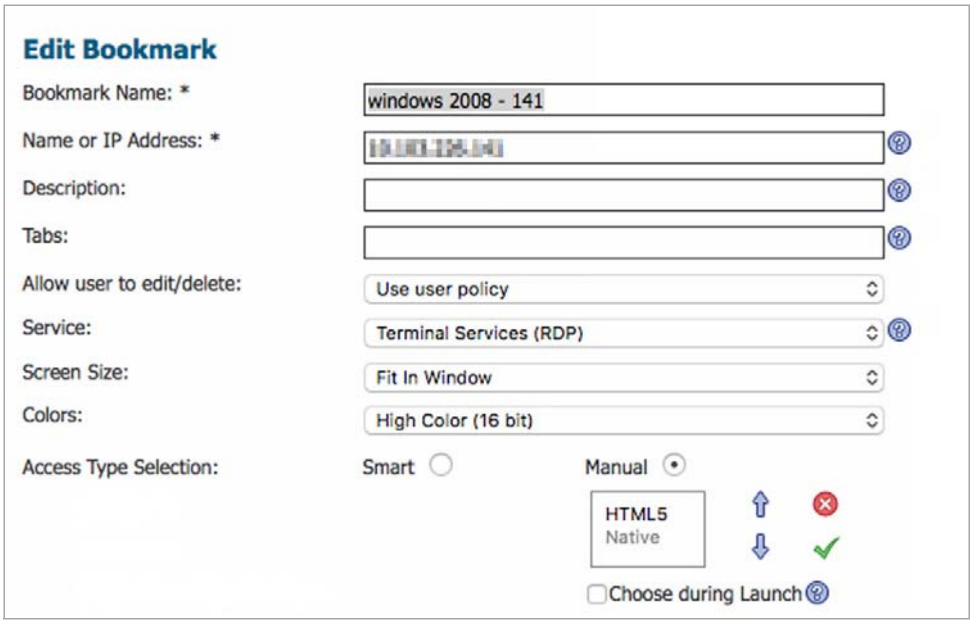
□ Use Login Domain for SS

○ Use custom credentials

□ Forms-based Authentication

□ Display Bookmark to Mobile Conn

When adding or editing RDP/VNC/SSH/Telnet bookmarks in the launch method area, any Java association will be removed. If there is only one launch method in use, the “Access Type Selection” options are hidden as well.



Edit Bookmark

Bookmark Name: * windows 2008 - 141

Name or IP Address: * [redacted]

Description:

Tabs:

Allow user to edit/delete: Use user policy

Service: Terminal Services (RDP)

Screen Size: Fit In Window

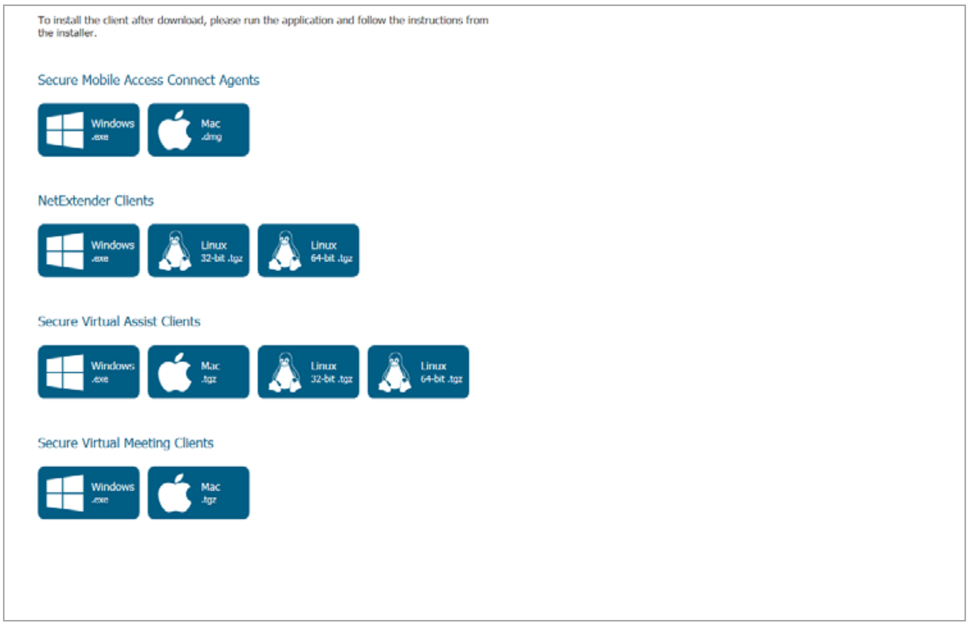
Colors: High Color (16 bit)

Access Type Selection: Smart ○ Manual ●

Moving clients from the firmware to the backend server

In SMA 8.6.0.1, all clients are being moved from the firmware to the backend server. During bootup, the firmware syncs and downloads the clients to the backend server from the firmware creating more space in the firmware.

When clients are not available, the downloaded clients page appears as:



To install the client after download, please run the application and follow the instructions from the installer.

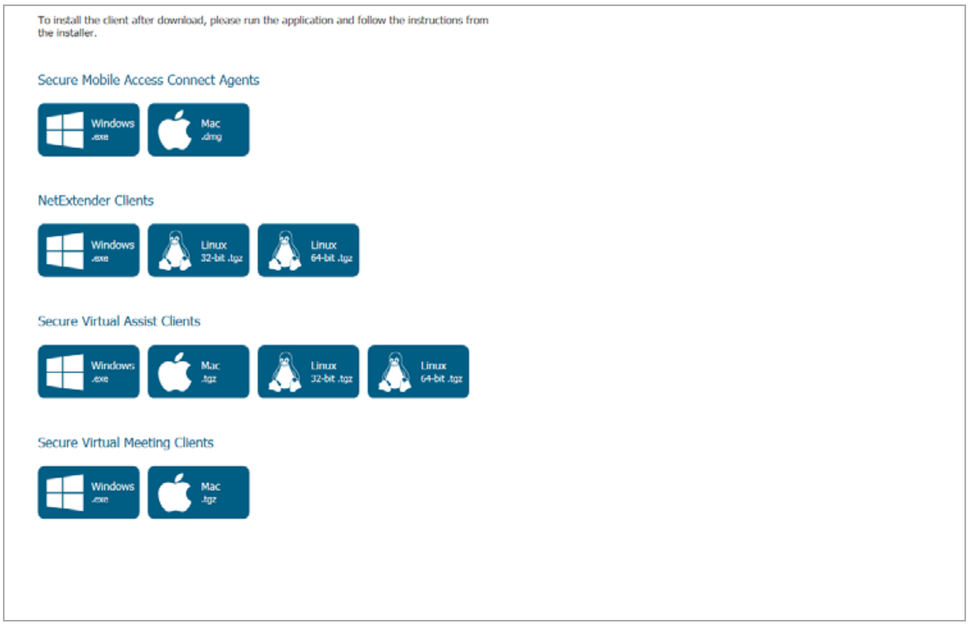
Secure Mobile Access Connect Agents

NetExtender Clients

Secure Virtual Assist Clients

Secure Virtual Meeting Clients

When the clients are available, the clients downloaded page appears as:



To install the client after download, please run the application and follow the instructions from the installer.

Secure Mobile Access Connect Agents

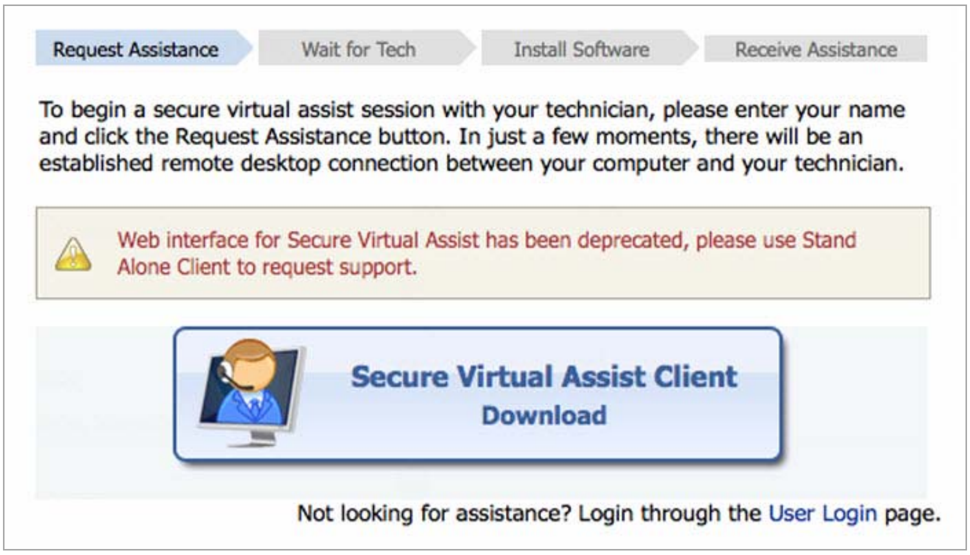
NetExtender Clients

Secure Virtual Assist Clients

Secure Virtual Meeting Clients

Deprecating the VirtualAssist and VirtualMeeting web interfaces

In SMA 8.6.0.1, you can no longer request support from the web interface using the support login CGI for Secure Virtual Assist.



To begin a secure virtual assist session with your technician, please enter your name and click the Request Assistance button. In just a few moments, there will be an established remote desktop connection between your computer and your technician.

Web interface for Secure Virtual Assist has been deprecated, please use Stand Alone Client to request support.

Not looking for assistance? Login through the User Login page.

The Virtual Meeting web interfaces have been removed as well.

Resolved issues

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

Vulnerability

Resolved issue	Issue ID
Before version 4.5, Linux Kernels inadvertently allowed remote attackers to execute arbitrary code by way of UDP traffic, which triggered an unsafe second checksum calculation during the execution of the recv system call with the MSG_PEEK flag.	185894

HTML5

Resolved issue	Issue ID
Application fails to load properly. Occurs when launching an HTML5 bookmark.	186012

Logs

Resolved issue	Issue ID
Device Management fails when attempting to remove log files from Device Management. Files cannot be removed. Occurs when Device Management logs a user’s connection.	186010

Services

Resolved issue	Issue ID
Application path does not function correctly. Occurs when using Native bookmarks.	186011

System

Resolved issue	Issue ID
Added an option to control the session life cycle.	184915

Known issues

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

Endpoint control

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

HTML5

Known issue	Issue ID
The HTML5 RDP with broker redirection fails. Occurs when using Edge or Internet Explorer 11 with Windows 10. Workaround: Utilize Chrome or Firefox.	186025

SSL-VPN

Known issue	Issue ID
The MAC SMA Agent upgrade fails. Occurs when the appliance is updated from build 8.5 to 8.6. Workaround: Uninstall and reinstall the SMA Agent for MAC systems when impacted.	186083
NetExtender does not appear. Occurs when trying to connect from the portal.	186073

System compatibility

Topics:

- Feature support by platform
- NetExtender client versions
- Virtual Assist and Virtual Meeting client versions

Feature support by platform

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

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

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

- Load Balancing

Features not supported on SMA 200 and SRA 1600

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

- Application profiling
- High Availability
- Virtual Meeting

NetExtender client versions

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

Description	Version
NetExtender Linux RPM 32-Bit	8.6.800-1
NetExtender Linux RPM 64-Bit	8.6.800-1
NetExtender Linux TGZ 32-Bit	8.6.800
NetExtender Linux TGZ 64-Bit	8.6.800
NetExtender MacOSX	8.5.788
NetExtender Windows	8.6.258

Virtual Assist and Virtual Meeting client versions

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

Description	Version
Virtual Assist Linux RPM	8.6.x
Virtual Assist Linux TGZ	8.6.x
Virtual Assist MacOSX	8.6.0.1
Virtual Assist Windows	8.6.0.5
Secure Virtual Meeting MacOSX	8.6.0.1
Virtual Meeting Windows	8.6.0.6

Product licensing

The SonicWall Secure Mobile Access 8.6.0.1 firmware provides user-based licensing on SonicWall SMA/SRA appliances. Licensing is controlled by the SonicWall license manager service, and you can add licenses through their MySonicWall accounts. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWall.

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

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

To activate licensing for your appliance:

1 Log in as admin, and navigate to the **System > Licenses** page.

2 Click the **Activate, Upgrade or Renew services** link. The MySonicWall login page is displayed.

3 Type your MySonicWall account credentials into the fields to log into MySonicWall. This must be the account to which the appliance is, or will be, registered. If the serial number is already registered through the MySonicWall web interface, you will still need to log in to update the license information on the appliance itself.

   MySonicWall automatically retrieves the serial number and authentication code.

4 Type a descriptive name for the appliance into the **Friendly Name** field, and then click **Submit**.

5 Click **Continue** after the registration confirmation is displayed.

6 Optionally upgrade or activate licenses for other services.

7 After activation, view the **System > Licenses** page on the appliance to see a cached version of the active licenses.

Upgrading information

See the *SonicWall™ Secure Mobile Access Upgrade Guide* at SMA Documentation.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/contact-support.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' 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 SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME 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 SONICWALL AND/OR ITS AFFILIATES 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 SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal/.

Legend

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

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

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

Last updated: 4/25/17

232-003815-00 Rev A