SonicWall® Secure Mobile Access 12.3

Workplace User Guide

SONICWALL®

Contents

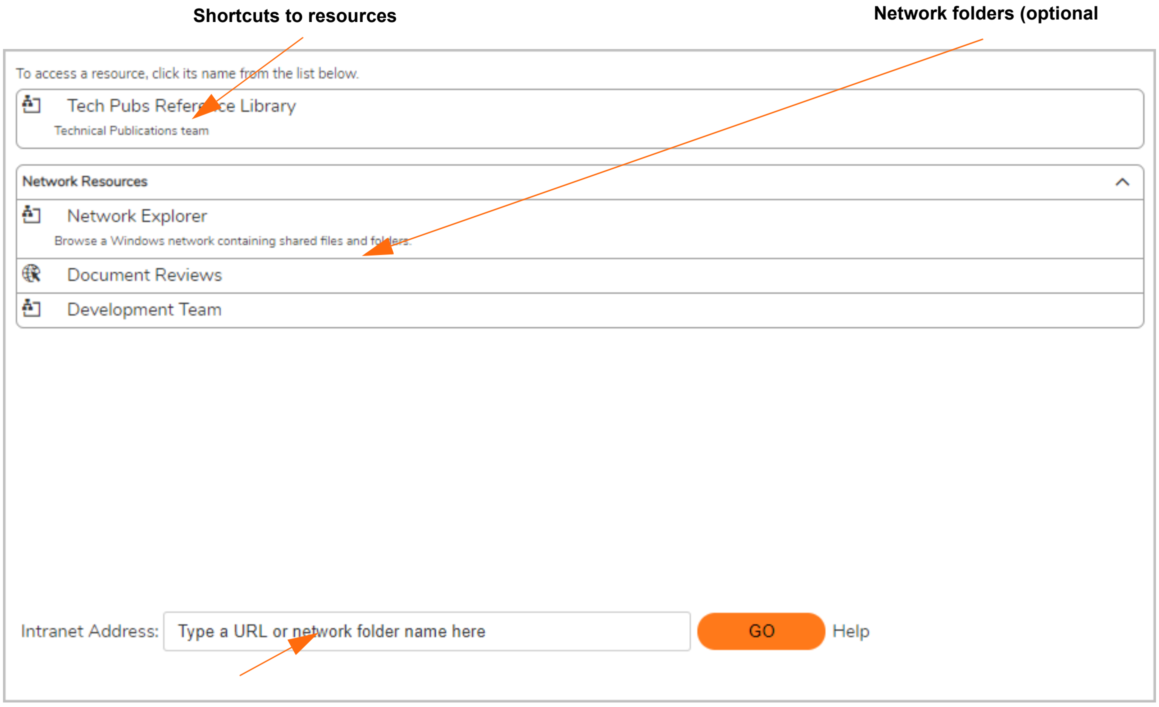
1

Using Secure Mobile Access WorkPlace

The WorkPlace application enables you to securely access private network resources—including Web sites, Web and client/server applications, terminal servers, and shared folders or files—from a Web browser.

WorkPlace Overview

When you start WorkPlace, the home page displays any shortcuts that your administrator has configured for you. You can click these links for direct access to Web content, applications, or shared folders and files. Some elements, such as the Network Explorer page, personal bookmarks, or the **Intranet Address** box, may not be available depending on how the home page is configured.



To access a resource, click its name from the list below.

Tech Pubs Reference Library
Technical Publications team

Network Explorer
Browse a Windows network containing shared files and folders.

Document Reviews

Development Team

Type a URL or network folder name here

Your WorkPlace pages may look different than the examples shown in this document. If your SonicWall SMA appliance was upgraded after version 10.6.2, by default the WorkPlace pages are displayed in the format used in previous versions. The administrator can update the WorkPlace to the new format, but doing so resets the WorkPlace pages to the factory default.

The WorkPlace home page includes connection status information indicating which access methods are currently enabled and the session start time. You can click the **Details** link in this area to view your security zone status (if applicable) and see information that can be helpful in troubleshooting problems. For more information about access methods, see Access Methods and Resources. For more information about security zones, see Viewing Security Zone Information.

Depending on how your administrator has configured WorkPlace and how you connect to the network, the home page may include a **Personal Bookmarks** area that enables you to save and access your own collection of links to URLs and other resources, such as file shares. To manage your bookmarks, click the pencil icon. For more information, see Using Bookmarks.

ⓘ **NOTE:** To navigate to and from different pages in WorkPlace, use the navigation tools in WorkPlace (tabs or links) instead of your Web browser's **Back** and **Forward** buttons. Clicking the browser's navigation buttons prompts you to terminate your WorkPlace session.

The Network Explorer Page

Your system administrator can make the Network Explorer page available to you, giving you access to all the Windows network folders or files for which you have permissions. There are two versions of Network Explorer: the HTML-based file explorer, and the Java-based version.

- In the HTML-based Network Explorer, the navigation pane at the left displays a list of resources available on your network; the pane on the right enables you to work with folders and files.
- The Java-based Network Explorer displays the file system on the local machine in the left pane and the remote location in the right pane. The right pane allows you to browse network domains and computers, and their associated file shares. Using the two panes, you can manipulate files and copy between the remote and local file systems. Users can also set up bookmarks from within Network Explorer to quickly navigate through networks from the portal level.

Access Methods and Resources

WorkPlace enables you to access different types of resources. The specific resources available depend on the access methods currently enabled, as shown in the connection status area in WorkPlace. The following table describes the various access methods and the types of resources each one enables you to access.

Access methods and resources

Access method	Resources available
Web	• Web content and Web-based applications that can be accessed through a browser. Examples include general Web sites (such as intranets), Outlook Web Access, and Domino Web Access.
Web and client/server	• Web content and Web-based applications that can be accessed through a browser. • Client/server applications, thin client applications, and terminal servers. Examples include Outlook, Citrix, and Windows Terminal Services.
Full network access	• Web content and Web-based applications that can be accessed through a browser. • Client/server applications, thin client applications, and terminal services. • Native Windows file access through Network Neighborhood. • Mapped network drives.

For more system status information, click **Details**, which provides access to the following features:

- Session information - Identifies the Realm, Community, and whether Data Protection is being used.
- SMA Agents - Identifies the SMA agents are available on your device and what security zone (community) you have been assigned to. Your system administrator may also make WorkPlace shortcuts available that allow you to download and install additional clients (for example, Connect Tunnel and Connect Mobile).
- Secure Endpoint Manager - Identifies the version of Secure Endpoint Manager being used.
- Device Authorization Terms - Provides an Authorization Terms and consent form to allow access to the network resources from a personal device.

Logging into WorkPlace

Before you can access your WorkPlace resources, your identity must be verified. Depending on how your administrator has configured WorkPlace, this might mean selecting a specific login group (for example, “Employees” or “Partners”), and then providing credentials. You may be prompted for a username and password, which you can type in or enter by means of a virtual keyboard, or you may be prompted for some other form of credentials.

1. If you are presented with a **Please log in** prompt, select the appropriate group from the list. (This information is provided by your system administrator.) If the list does not contain the appropriate name, select *Other* from the list, and then type the group name in the box below the **Log in to** box.
2. Click **Next**.
3. If configured by your administrator, the Acceptable Use Policy screen (AUP) appears. The AUP displays specific messages or instructions you will need to agree to. Click **Accept** to continue. If you do not accept the license agreement, you will not be able to access WorkPlace.
4. If logging in with a personal device for the first time Device Authorization Terms are displayed. Read and agree to the terms to login.
5. When prompted for credentials, enter them, and then click **Login**.

   Your administrator can offer an alternative method for providing your credentials using a virtual keyboard. Some administrators may even require it if, for example, there is concern that a user’s login credentials might be stolen. To enter your credentials without typing them, click **Use virtual keyboard** and point to characters on the keyboard display.

   ⓘ **NOTE:** Keyboard entry may not be accepted when using RDP in full screen mode on Mac OS X.

6. If CAPTCHA authentication is enabled for your realm, a CAPTCHA verification display and prompt appear. Type the 6-character case sensitive alphanumeric CAPTCHA value. To view a different CAPTCHA, click the **New** button.
7. Windows users are prompted to install the Secure Endpoint Manager (SEM), which takes care of installing agents and clients through the browser. Once it is installed, you automatically receive client updates. Click **Continue**, then click **Run** and accept the software if any security warnings appear.
   - The URL you use to log in to WorkPlace is provided by your system administrator.
   - Depending on how your administrator has configured WorkPlace, all other open browser windows may automatically close at WorkPlace startup, leaving only the WorkPlace browser window open.
   - Your administrator can configure the SEM to start automatically when the operating system starts (Windows only).
   - In some cases, you may be prompted to accept a security warning before WorkPlace can start. For more information, see Using Cache Cleaner.

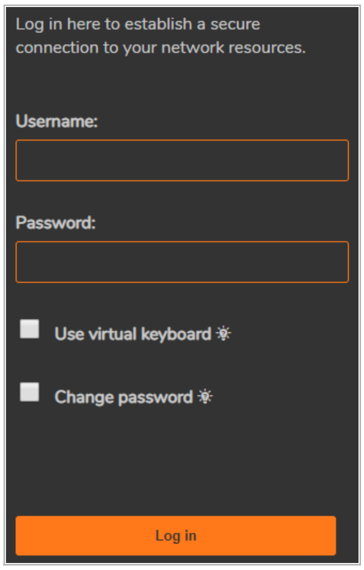
Topics:

- Changing Your Password
- Entering Credentials Using the Virtual Keyboard

Changing Your Password

Your administrator has the option of allowing you to change your own password in WorkPlace.

If a user-initiated password change is allowed, you'll see the **Change password** checkbox



Log in here to establish a secure connection to your network resources.

Username:

Password:

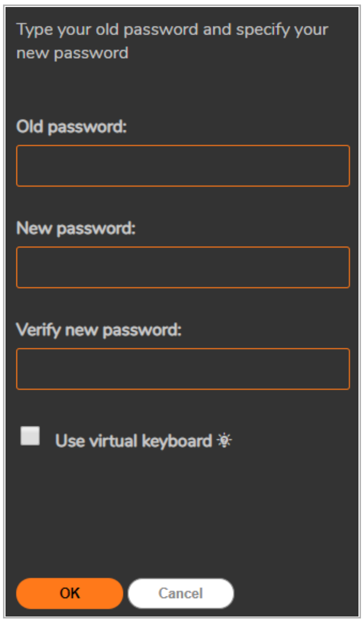
□ Use virtual keyboard

□ Change password

To change your password:

1 Click **Change password**.

2 Enter your current credentials, and then click **Log in**.



Type your old password and specify your new password

Old password:

New password:

Verify new password:

□ Use virtual keyboard

3 Re-enter your old password.

4 Enter your new password.

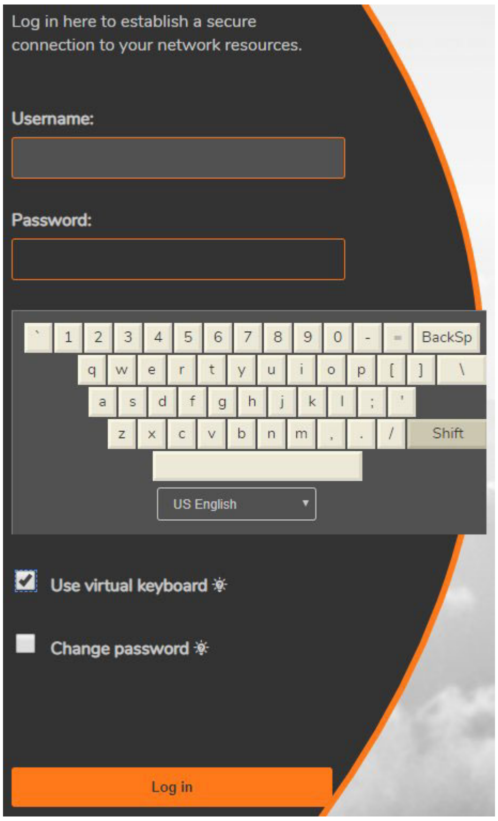
5 Re-enter your new password.

6 Click **OK**.

Entering Credentials Using the Virtual Keyboard

The administrator can offer you an alternative method of providing your credentials in WorkPlace using a virtual keyboard. Some administrators will require it if, for example, there is concern that a user's login credentials might be stolen.

1 Click the **Use virtual keyboard** checkbox: a keyboard is displayed in WorkPlace. (If your administrator requires that you use the virtual keyboard, it is already displayed.)



Log in here to establish a secure connection to your network resources.

Username:

Password:

☑ Use virtual keyboard

□ Change password

` 1 2 3 4 5 6 7 8 9 0 - = BackSp
q w e r t y u i o p [ ] \
a s d f g h j k l ; '
z x c v b n m , . / Shift
US English
Log in

2 Click the letters for the username. To enter a capital letter, first click the Shift key on the virtual keyboard.

3 Use your mouse to move the cursor to the password box, and then click the letters for your password.

Logging out of WorkPlace

When you have finished working with network resources using WorkPlace, you should log out to close your session.

To log out, click the **Log out** button in the upper-right area of the WorkPlace page.

> **NOTE:** Logging out of WorkPlace ends your WorkPlace session, but it does not log you out of any applications that are running on your computer. To increase security, it is good practice to close any browser windows in use by applications before you log out of WorkPlace, especially if you are working on a computer that is shared with other users.

WorkPlace Lite

WorkPlace Lite is an access mode for the Secure Mobile Access (SMA) appliance that bypasses all Access and EPC Agents and logs the user in to WorkPlace. The only prerequisite for logging in to a WorkPlace Lite enabled WorkPlace site as a modern web browser that supports HTML5. Web only access is more commonly referred to as Reverse Proxy access.

The AMC administrator can:

- Grant the user access to WorkPlace Lite.
- Force the user to use WorkPlace Lite only.
- Disable the user from accessing WorkPlace Lite.

Users can select a checkbox or go to a specific WorkPlace site for Lite access. If the user checks WorkPlace Lite mode, then the system allows access to browser based graphical and text-terminal shortcuts as well as Web URL and HTML file share shortcuts. The Persistent Cookie option allows (or disallows) seamless access to SharePoint documents.

Accessing Network Resources

You can use several methods to access a specific resource. Depending on how your administrator has configured WorkPlace, some access methods may not always be available.

- **Shortcuts:** The WorkPlace home page displays any shortcuts that your administrator has configured for you. You can click these links to directly access selected web applications, network shares or folders, or terminal servers. For more information, see Using Shortcuts.
- You can use the **Intranet Address** box at the bottom of the page to access a web resource, a network resource, or a terminal server. For more information, see Using the Intranet Address Box.
- **Personal Bookmarks:** You may be able to create your own bookmarks for quick access to resources such as URLs and file shares. For more information, see Using Bookmarks.
- **Access methods:** To find out what access agents are running, click **Details** in WorkPlace. Your administrator may also make client installation packages available for download. For more information, see Access Methods and Resources.
- **Browsing network resources:** You can use the WorkPlace Network Explorer page to browse a Windows network, including shared folders and files. For more information, see Working with Folders and Files.

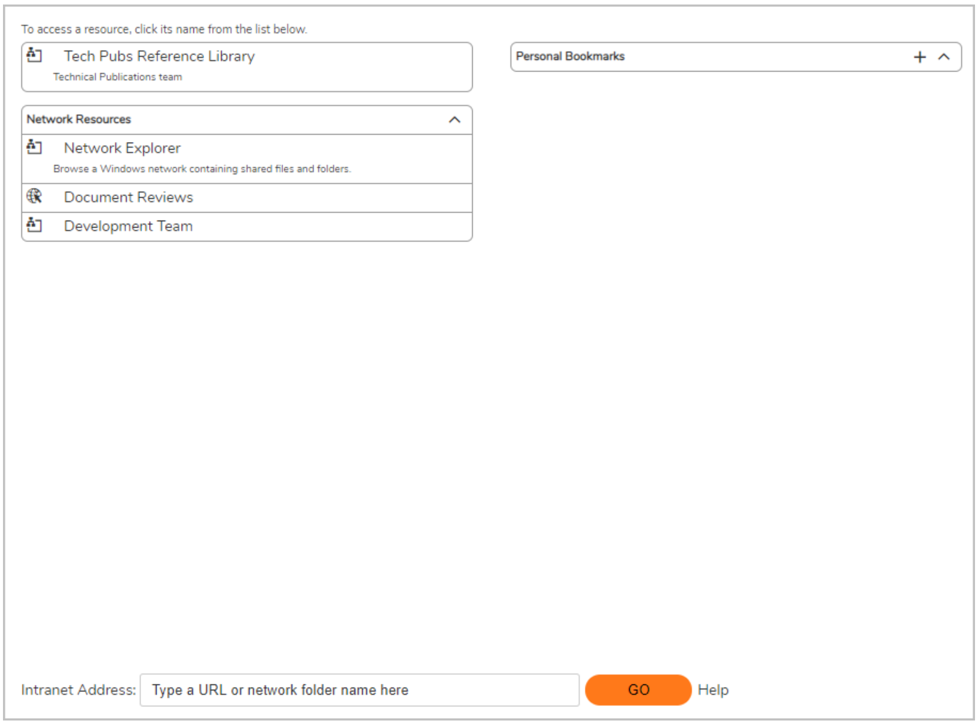
ⓘ **NOTE:** Accessing some items may require you to log in if special permissions are required for that item. WorkPlace first attempts to access network share resources using your WorkPlace login credentials; if the resource requires different credentials, you are prompted to supply them.

Related Topics

- Using Shortcuts
- Using the Intranet Address Box
- Using Bookmarks

Using Shortcuts

WorkPlace shows the shortcuts that your administrator configured for you. How they are organized—in groups, or on different pages—is defined by your administrator. You can click these links to directly access Web content, applications, shared folders, terminal servers, and Workspace Server Farm resources.



To access a resource, click its name from the list below.

Tech Pubs Reference Library
Technical Publications team

Network Resources

Network Explorer
Browse a Windows network containing shared files and folders.

Document Reviews

Development Team

Personal Bookmarks

Intranet Address: Type a URL or network folder name here

You can edit several of the shortcuts. Any changes you make will be used every time you click the shortcut for that resource. If you do not make any changes, the settings defined by your administrator is used. The editable shortcuts include:

- Windows Terminal Services
- Citrix and Citrix graphical terminal shortcuts
- SSH/Telnet (text terminal shortcuts)
- VNC
- RDP

To create a custom shortcut, refer to To Configure Custom Links.

To Access a Resource Using a Shortcut

Click the shortcut name for the resource you want to access. Web resources and terminal server resources open in a new browser window. The vWorkspace desktop and shared folders or files open in a separate Network Explorer window. Clicking a vWorkspace server farm shortcut displays a window identifying its applications and desktops, similar to Citrix and VMware server farm bookmarks.

ⓘ **NOTE:** If using Google Chrome to access a Web resource and a blank page appears, disable the **Use hardware acceleration when available** option in Google Chrome.

To Configure Custom Links

Click the **Edit** icon for the resource shortcut to open the **Add Shortcut** dialog box.

1 Select the **Client Type** drop-down list.

2 Select one of the following from the **Screen resolution** drop-down list and then click **Save**:

- To use a resolution in the list, select the desired resolution.
- To create a custom resolution, select **Custom...** and then type the desired pixel values (width x height) into the fields that appear.
- To set the resource window size as a percentage of your client screen, select **Screen Percent** and then type the desired percentage into the **percent** field that appears.
- To use your full screen to display the resource, select **Full Screen**.

3 Select the desired color depth from the **Color Depth** drop-down list. Possible choices are 8-bit, 24-bit, 32-bit, and 64-bit color. The default value is 16-bit.

4 Select a **Connection type**.

5 Select a **Keyboard layout**.

6 To allow connecting to the admin/console session, select **Connect to admin/console session**.

7 Select **Enable Single Sign On** and choose the type of credentials to be used:

- To use the same credentials used to login to the WorkPlace session, select **Use WorkPlace session credentials**.
- To use custom credentials, select **Use custom credentials** and type the **Username**, **Password**, and **Domain** to use for logging in.

8 To allow the use of multiple displays, select **Enable multi-monitor support**.

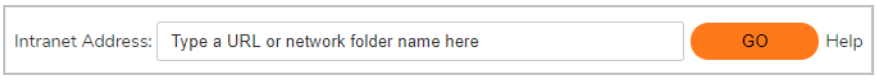
9 To allow the use of third-party DLLs, select **Enable third-party plugin DLLs**.

10 To enable Wake on LAN, select **Enable Wake-on-LAN (WoL)**.

11 Click **Save**.

Using the Intranet Address Box

Depending on how your administrator has configured WorkPlace, you may see an **Intranet Address** box, which you can use to access network resources, terminal server resources, or, when WorkPlace is running in translated mode, Web resources.



ⓘ **NOTE:** If using Google Chrome to access a Web resource and a blank page appears, disable the **Use hardware acceleration when available** option in Google Chrome.

Topics:

- Accessing Web Resources Using the Intranet Address Box
- Accessing Network Resources Using the Intranet Address Box
- Accessing Terminal Servers Using the Intranet Address Box

Accessing Web Resources Using the Intranet Address Box

To access a Web resource, type the URL for the resource in the **Intranet Address** box, and then click **GO**. The Web resource opens in a new browser window. Remember the following:

- If you are accessing a standard HTTP resource, you do not need to type `http://` at the beginning of the URL. However, if you are accessing a secure Web (HTTPS) resource, you must include the `https://` protocol identifier in the URL (`https://intranet.example.com`).
- To access a Web resource on a non-standard port (other than port 80), include the port number after the resource's host name. For example, `intranet.example.com:443` and `intranet.example.com:8080/SAP` are both valid entries.

Accessing Network Resources Using the Intranet Address Box

To go directly to a server, computer, or network folder, type the item's path in the **Intranet Address** box, and then click **GO**. Network Explorer opens in a new browser window, displaying the contents of the requested folder or file.

When specifying a resource name, use the Windows Universal Naming Convention (UNC) name, in the format \\ComputerName\ShareName\Path\FileName. For example, to view the contents of the \sales\proposals folder on the *common* server, type the following in the **Intranet Address** box:

```
\\common\sales\proposals
```

When using the Internet Address Box:

- WorkPlace does not support unqualified host names for network resources; you must type the full UNC name when entering a network resource name in the **Intranet Address** box.
- Typing an unqualified host name in the **Intranet Address** box is interpreted as a Web resource, not a network resource. For example, if you have a Web resource named *intranet.example.com*, simply type `intranet` in the **Intranet Address** box to access it.

Accessing Terminal Servers Using the Intranet Address Box

To go directly to a terminal server resource, type its URL in the **Intranet Address** box, and then click **GO**. The resource opens in a new browser window.

When specifying a terminal server resource URL, you must include the appropriate protocol identifier. If a terminal server resource contains multiple hosts, you are prompted to type the host name or IP address of the specific resource you want to access.

Terminal server resource data

Terminal server type	Identifier	Sample Intranet Address box entry
Windows Terminal Services	`rdp://`	`rdp://private.xyzcompany.com/wts_server`
Citrix	`citrix://`	`citrix://private.abccompany.com/citrix_farm`

Options Using HTML5

Topics

- Overview
- RDP Using HTML5

Overview

HTML5 clients can connect to backend systems using RDP, VNC, SSH, and Telnet. HTML5 clients can use Single Sign-On (SSO), copy and paste, multiple language keyboard support, scroll back, and dynamic window resizing. Users also have wider connectivity, such as cross-browser, cross-OS support.

NOTE: RDP, VNC, SSH, and Telnet usng HTML5 can be configured in SMA 12.3 on an SMA 1000 series appliance or in SMA 12.3 WorkPlace.

HTML5 clients eliminate the management of the endpoint clients, such as Java and ActiveX. The following table shows the HTML5 features for RDP, VNC, SSH, and Telnet:

RDP	**SSH and Telnet**	**VNC**
Keyboard - AMC Support	SSO	SSO
Keyboard enhancements	Scroll back	Performance improvements for Mac screen sharing
TLS/NLA - AMC Support	Dynamic Window Resize (remove Window size AMC option)	Window Control
RDP Certificate identity warning		
Copy-Paste	Copy-Paste	Copy-Paste, Encoding, Compression Level, JPEG iMage Quality, Cursor Shape Update, Use CopyRect, Restricted Colors, View Only, Share Desktop
Optimize for tablets/phones	Zoom-in and Zoom-out	
Per Device License	Host Key - SSH default font size	

RDP Using HTML5

Topics

- Keyboard Support for RDP
- Copy and Paste in HTML5 RDP

NOTE: Server authentication for RDP is configured by the system administrator.

Keyboard Support for RDP

Keyboard support for WorkPlace and AMC has been enhanced with support for additional languages. You can select the keyboard language from a drop-down menu in WorkPlace and in AMC. The language that the browser is set to, is used as the default keyboard language.

These keyboard languages are supported in SMA 12.3:

Bosnian (Cyrillic, Bosnia, Herzegovina)
Bulgarian
Croatian
Czech
Danish
Dutch
English (United Kingdom, United States)
Finnish
French (Belgium, Canada, France, Switzerland)
German (Germany, Switzerland)
Greek
Hungarian
Irish
Italian
Lithuanian
Luxembourgish
Norwegian
Polish
Portuguese (Portugal)
Romanian
Russian
Spanish
Swedish
Turkish

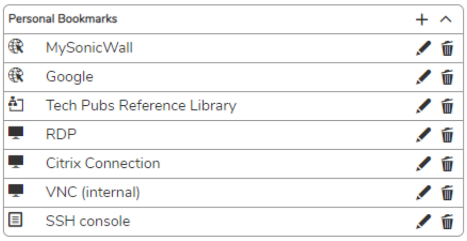
Copy and Paste in HTML5 RDP

You can copy and paste text from one RDP device to another as follows:

- Local to local
- Local to Remote
- Remote to local

Using Bookmarks

Depending on how your administrator has configured WorkPlace, the home page may include an area where you can save and access personal links to resources such as URLs and file shares.



Personal Bookmarks

- MySonicWall
- Google
- Tech Pubs Reference Library
- RDP
- Citrix Connection
- VNC (internal)
- SSH console

NOTE: Bookmarks are not supported when using Application Access Control.

WorkPlace bookmarks are similar to standard Web browser bookmarks or favorites lists, except that they are stored on the SonicWall SMA appliance, not on a specific computer. You can access and manage your WorkPlace personal links whenever you are logged in to WorkPlace, regardless of the computer you are using. When you click a bookmark, the specified resource opens in a separate browser window.

NOTE: To access file shares through WorkPlace bookmarks, you must be running a SonicWall SMA access agent, such as one of the tunnel clients, or you must configure the bookmark to use a special URL. For more information, see Adding Bookmarks, or contact your system administrator.

NOTE: If using Google Chrome to access a Web resource and a blank page appears, disable the **Use hardware acceleration when available option** in Google Chrome.

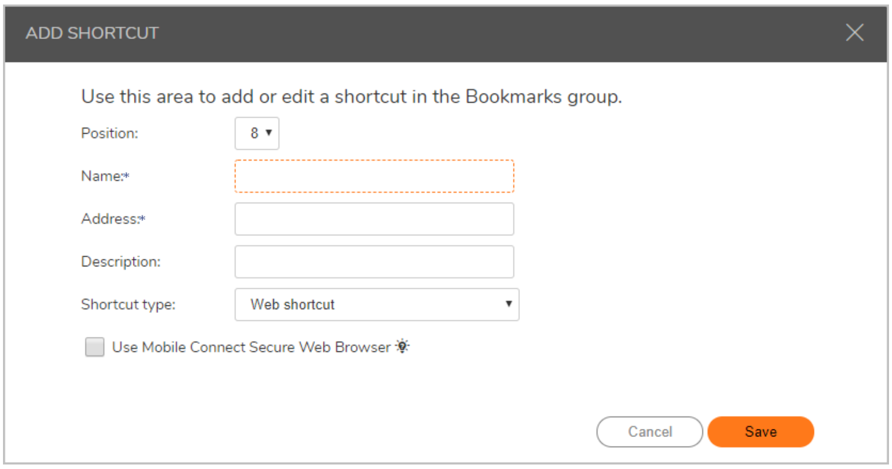
Topics:

- Adding Bookmarks
- Reordering Bookmarks
- Editing Bookmarks
- Deleting Bookmarks

Adding Bookmarks

After you add a bookmark, it appears in the **Personal Bookmarks** group in WorkPlace.

1 In the **Personal Bookmarks** group in WorkPlace, click the **plus** icon. The **Manage bookmarks** page appears.



ADD SHORTCUT

Use this area to add or edit a shortcut in the Bookmarks group.

Position: 8

Name:*

Address:*

Description:

Shortcut type: Web shortcut

□ Use Mobile Connect Secure Web Browser

2 For **Position**, select the position for where the bookmark will appear in the list of bookmarks on the WorkPlace page.

3 In the **Name** field, type a short, descriptive name for the bookmark. This name will appear as the link text in the **Personal Bookmarks** group in WorkPlace.

4 In the **Address** field, type the URL or path for the resource:

- To create a bookmark for a URL, type the URL in *host/path* format. If you are creating a bookmark for a standard HTTP resource, you do not need to type `http://` in the URL. However, if you are creating a bookmark for a secure Web (HTTPS) resource, you must include the `https://` protocol identifier in the URL (`https://intranet.example.com`).
- To create a bookmark for a file share resource, type the file share path in Windows Universal Naming Convention (UNC) format (\\*ComputerName**ShareName**Path**File*). For example, to add a bookmark for the *sales**proposals* folder on the *common* server, type `\\common\sales\proposals`.

5 In the **Description** field, type in a short description for the resource.

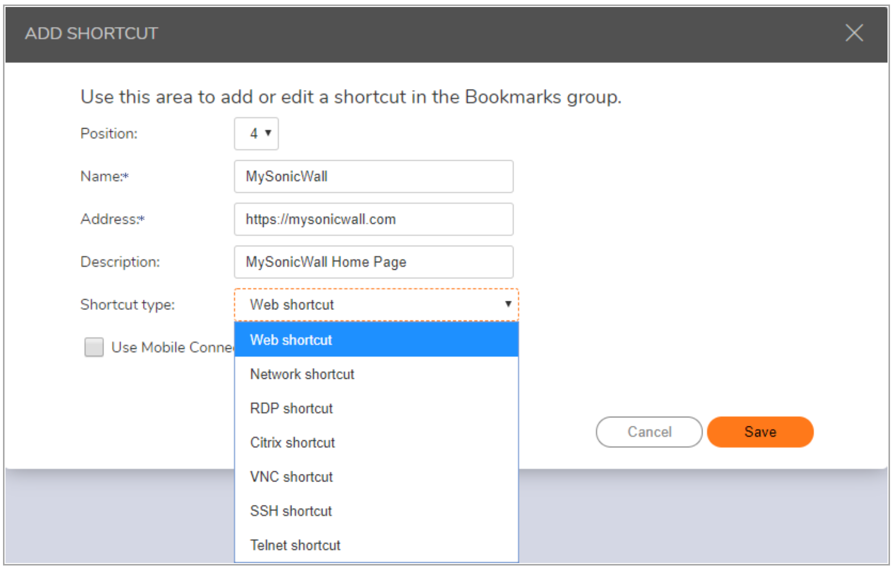
6 Select the type of shortcut from the **Shortcut Type** drop-down list. Choose one of the following:

- Web shortcut
- Network shortcut
- RDP shortcut
- Citrix shortcut

- VNC shortcut
- SSH shortcut
- Telnet shortcut

The display changes depending on what you select.

For example, a Web shortcut might be configured as shown below:



ADD SHORTCUT

Use this area to add or edit a shortcut in the Bookmarks group.

Position: 4

Name:* MySonicWall

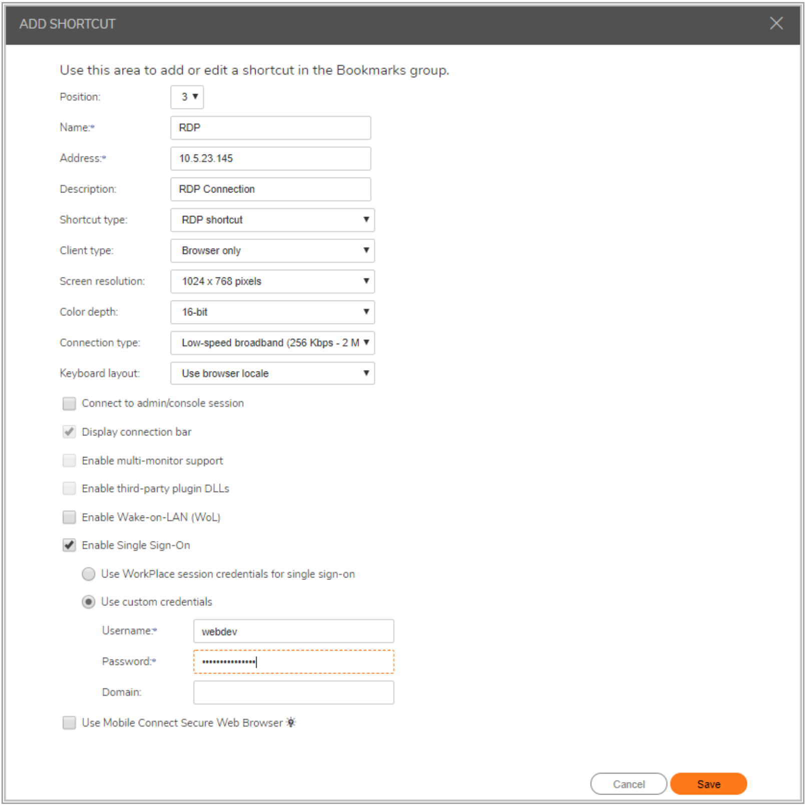
Address:* https://mysonicwall.com

Description: MySonicWall Home Page

Shortcut type: Web shortcut

□ Use Mobile Conne

An RDP shortcut might be configured as shown below:



ADD SHORTCUT

Use this area to add or edit a shortcut in the Bookmarks group.

Position: 3

Name:* RDP

Address:* 10.5.23.145

Description: RDP Connection

Shortcut type: RDP shortcut

Client type: Browser only

Screen resolution: 1024 x 768 pixels

Color depth: 16-bit

Connection type: Low-speed broadband (256 Kbps - 2 M

Keyboard layout: Use browser locale

□ Connect to admin/console session

☑ Display connection bar

□ Enable multi-monitor support

□ Enable third-party plugin DLLs

□ Enable Wake-on-LAN (WoL)

☑ Enable Single Sign-On

○ Use WorkPlace session credentials for single sign-on

● Use custom credentials

Username:* webdev

Password:* •••••••••••••••

Domain:

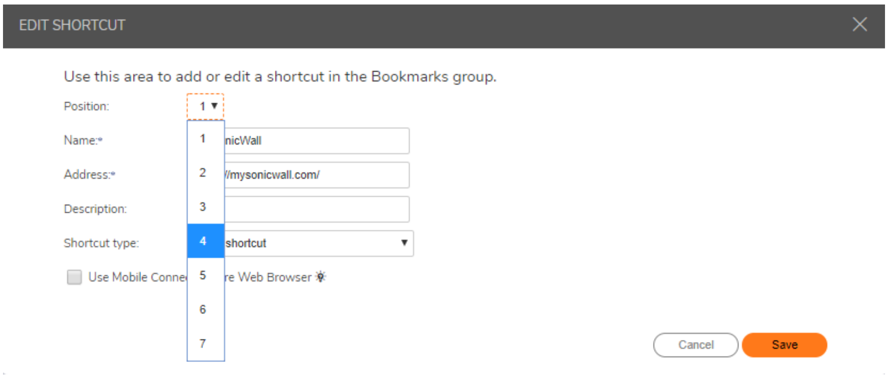
□ Use Mobile Connect Secure Web Browser

7 Click **Save**.

Reordering Bookmarks

You can control the order of your bookmarks (for example, to place the most frequently used bookmarks at the top of the list).

1 In the **Personal Bookmarks** group in WorkPlace, click the pencil icon. The **Edit Shortcut** dialog appears.



EDIT SHORTCUT

Use this area to add or edit a shortcut in the Bookmarks group.

Position: 1

Name:* nicWall

Address:* /mysonicwall.com/

Description:

Shortcut type: shortcut

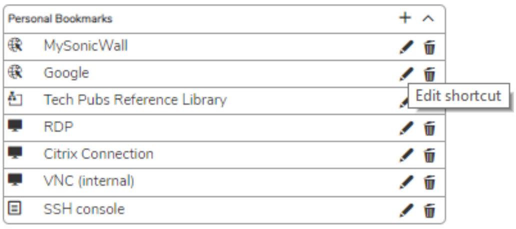
□ Use Mobile Conne re Web Browser

2 Select the desired position for this bookmark from the **Position** drop-down list.

3 Click **Save**.

Editing Bookmarks

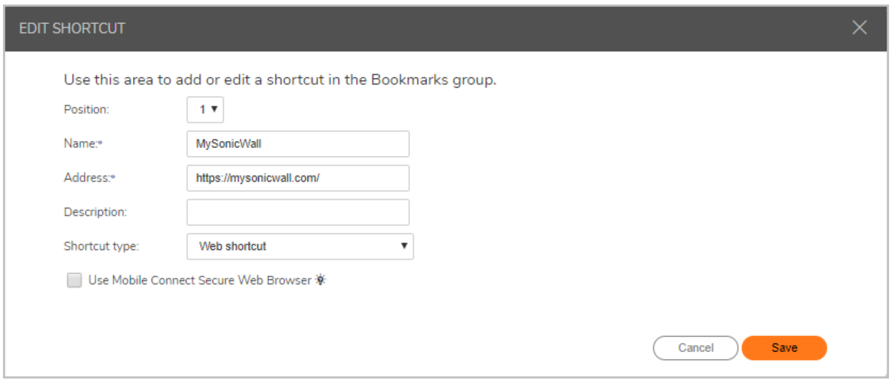
You edit bookmarks after you have added them.



Personal Bookmarks

- MySonicWall
- Google
- Tech Pubs Reference Library
- RDP
- Citrix Connection
- VNC (internal)
- SSH console

1 In the **Personal Bookmarks** group in WorkPlace, click the ✎ icon. The **Edit Shortcut** dialog displays.



EDIT SHORTCUT

Use this area to add or edit a shortcut in the Bookmarks group.

Position: 1

Name:* MySonicWall

Address:* https://mysonicwall.com/

Description:

Shortcut type: Web shortcut

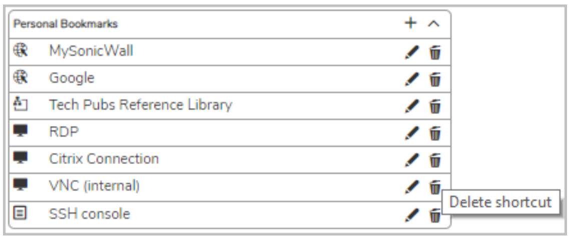
□ Use Mobile Connect Secure Web Browser

2 Edit the values that you want to change.

3 Click **Save**.

Deleting Bookmarks

You can delete bookmarks that you no longer need.



Personal Bookmarks

MySonicWall

Google

Tech Pubs Reference Library

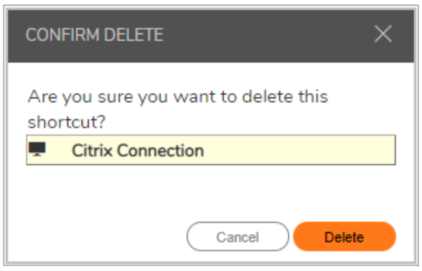
RDP

Citrix Connection

VNC (internal)

SSH console

1 In the **Personal Bookmarks** group in WorkPlace, click the ⊗ icon. The **Confirm Delete** dialog appears.



CONFIRM DELETE

Are you sure you want to delete this shortcut?

Citrix Connection

2 Click **Delete**.

Working with Folders and Files

WorkPlace enables you to work with network files and folders on a network using a Web browser much as if you were working locally on the network. To access file and folder utilities, click on Network Explorer.

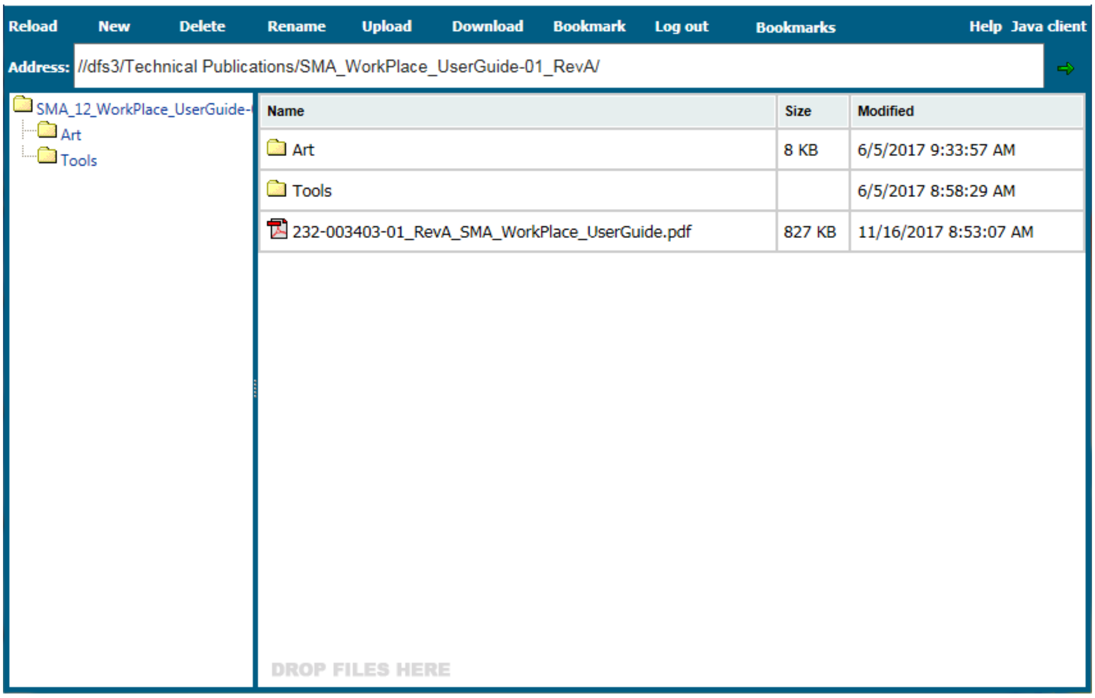
WorkPlace automatically displays the HTML-based Network Explorer, but there are two Network Explorer interfaces available:

- **HTML-based Network Explorer** – The HTML-based Network Explorer enables you to work with network files and folders on a network using a Web browser much as if you were working locally on the network. The Network Explorer page displays shared folders or files that you have permission to access, and provides access to file and folder utilities. You can use this Network Explorer to browse domains, servers, shares, folders, and files. The HTML-based Network Explorer is the default interface on all devices. See Using the HTML-Based Network Explorer.
- **Java-based Network Explorer** – The Java-based Network Explorer has a similar look and feel to the Windows Explorer tool, featuring drag and drop, multiple file selection, and bookmark capabilities. The interface displays the local computer in the left pane and the remote location in the right pane. See Using the Java-Based Network Explorer.

Using the HTML-Based Network Explorer

The HTML-based Network Explorer is the default interface on all devices. The HTML-based Network Explorer enables you to work with network files and folders on a network using a Web browser much as if you were working locally on the network. The Network Explorer page displays shared folders or files that you have permission to access. You can browse these domains, servers, shares, folders, and files by clicking links on the Network Explorer page. The navigation pane at the left displays a list of resources available on your network. The pane on the right enables you to work with folders and files.

ⓘ **NOTE:** Accessing some items may require you to log in, if special permissions are required for that item. WorkPlace first attempts to access network resources using your WorkPlace login credentials; if the resource requires different credentials, you are prompted to supply them.



Address: //dfs3/Technical Publications/SMA_WorkPlace_UserGuide-01_RevA/

Name	Size	Modified
Art	8 KB	6/5/2017 9:33:57 AM
Tools		6/5/2017 8:58:29 AM
232-003403-01_RevA_SMA_WorkPlace_UserGuide.pdf	827 KB	11/16/2017 8:53:07 AM

The File Share Controls describes the controls at the top of the File Share window.

File Share Controls

Button	Description
Reload	Reloads the current folder to display any changes.
New	Creates a new folder in the current network folder
Delete	Deletes the selected folder or folders. You will be prompted for confirmation before the folder are deleted.
Rename	Allows you to rename a selected folder or file.
Upload	Upload the selected files or folders to the selected network folder
Download	Download the selected files or folders to the local folder.
Bookmark	Creates a new bookmark to the current File Share location.
Logout	Logout of the File Share service.
Bookmarks	Displays a list of files and folders that you have bookmarked.

To update the contents of the navigation pane, click **Reload** on the top menu. This ensures that you are viewing the latest version of a network resource. For example, if you create a new file or folder and it does not show up in the navigation pane, click **Reload** to update the display.

Depending on your network environment, you may be able to access folders on your networked desktop computer, mobile device, etc. To do this, you must make those folders available using the Windows Sharing feature on that computer. See your Windows documentation for more information about sharing folders.

Related Topics

- Displaying the HTML Network Explorer Page
- Working with Folders
- Working with Files

Displaying the HTML Network Explorer Page

You can display the HTML Network Explorer page by doing one of the following (the methods available to you depend on how your administrator has configured WorkPlace):

- Click an appropriate network shortcut in WorkPlace.
- Type a UNC path name in the **Address:** box.

Working with Folders

When working with folders, you must have the correct permissions to perform certain actions; these are the same permissions you would need if you were working directly on the network. The folder page may include an option for uploading files from your computer to the current folder. For more information, see Uploading Files.

Topics:

- Viewing the Contents of a Folder
- Creating Folders
- Renaming Folders
- Deleting Folders

Viewing the Contents of a Folder

When you click a folder name, a page appears displaying that folder's contents. You can perform a number of different actions within the current folder, such as sorting items and creating, renaming, and deleting folders.

To view the contents of a folder:

1 Click the name of the folder you want to view in the left navigation pane of the Network Explorer page.

Any subfolders contained in the current folder are displayed in the left navigation pane. Any files contained in the current folder are displayed on the right.

Creating Folders

You can create a folder within the current folder.

1. In the left navigation pane of the Network Explorer page, click the name of the folder in which you want to create a new folder.
2. Click **New** from the top menu.
3. In the **New folder name** box, type the name of the folder you want to create.
4. Click **CREATE**.

Renaming Folders

You can rename the current folder.

1. In the right pane of the Network Explorer page, select the folder you want to rename.
2. Click **Rename** from the top menu. The name of the folder becomes editable.
3. Type a new name for the folder
4. Click the green checkmark icon.

Deleting Folders

You can delete the current folder. You are prompted to confirm before deleting the folder.

1. In the right pane of the Network Explorer page, click the name of the folder to delete.
2. Click **Delete in the top menu.**
3. Click the **DELETE** button to confirm that you want the folder deleted.

Working with Files

When working with files, you must have the correct permissions to perform certain actions; these are the same permissions you would need if you were working directly on the network.

Topics:

- Opening Files
- Downloading Files
- Uploading Files
- Renaming Files
- Deleting Files

Opening Files

You can open a file to display its contents; however, any changes that you make to the file will not be saved to the network. To modify the contents of a file, you must download a copy of the file to your computer, save your changes to the copied file, and then upload the new version of the file to the network.

To open a file, double-click the file that you want to open.

- web content opens in a new browser window
- other files open in their native applications.

If the application required to open a file cannot be found, you are prompted to save or open the file.

> ⓘ **NOTE:** Certain types of files, such as executable files or data files with proprietary file formats, must be downloaded or saved. They cannot be opened directly.

Downloading Files

You can download the current file to your local computer.

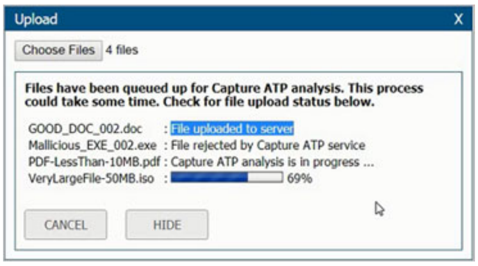
1. In the right pane of the Network Explorer page, click the file name of the file you want to download.
2. Click **Download** from the top menu. In most Web browsers, a dialog box appears prompting you to save or open the file.

Uploading Files

The folder page may include an option for uploading files from your computer to the current folder.

1. In the left navigation pane of the Network Explorer page, click the name of the folder to which you want to upload the files.
2. Click **Upload** from the top menu.
3. In the **Upload** box, click **Choose Files** to locate the files you want to upload from your computer.
4. Click **Open**. The files you selected will be uploaded to the folder you choose.

The files that you choose to be uploaded may be scanned for malicious behavior. If they are being scanned, the **Upload** box displays additional information about the uploading and scanning status of the files:



4 files

Files have been queued up for Capture ATP analysis. This process could take some time. Check for file upload status below.

```
GOOD_DOC_002.doc      : File uploaded to server
Mallicious_EXE_002.exe : File rejected by Capture ATP service
PDF-LessThan-10MB.pdf : Capture ATP analysis is in progress ...
VeryLargeFile-50MB.iso :              69%
```

- If the scanning of the files is successful, a message like this one is displayed:

GOOD_DOC_001.doc has been uploaded successfully.

- If the scanning of the files fails, a message like this one is displayed:

Capture ATP service has determined "Mallicious_EXE_001.exe" to be malicious, file has been rejected for upload. Please contact your administrator.

If this message is displayed, you should check your system for malicious or infected files.

Renaming Files

You can rename the current file.

1. In the right pane of the Network Explorer page, select the file you want to rename.
2. Click **Rename** from the top menu. The name of the file becomes editable.

3. Type a new name for the folder
4. Click the green checkmark icon.

Deleting Files

You can delete files from a folder. You are prompted to confirm the deletion.

To delete a file:

1. In the right pane of the Network Explorer page, click the name of the file you want to delete. The **File Details** page appears.
2. Click the **Delete file** button:
3. Click **Delete**.

Using the Java-Based Network Explorer

The Java-based Network Explorer displays the file system on the local machine in the left pane and the remote location in the right pane. The right pane allows you to browse network domains and computers, and their associated file shares. Using the two panes, you can manipulate files and copy between the remote and local file systems. Users can also set up bookmarks from within Network Explorer to quickly navigate through networks from the portal level.

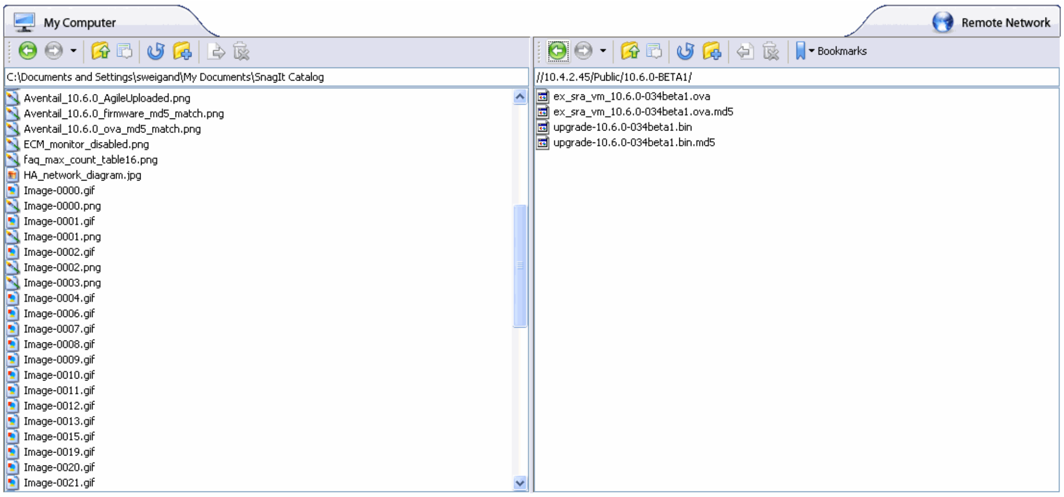
Network Explorer leverages the Java platform browser plug-in to increase usability by mimicking the common Windows Explorer interface, featuring drag and drop and multiple file selection capabilities. With the help of the HTTPS protocol, Network Explorer securely transfers encrypted files and information to and from the EX-Series appliance. The appliance communicates this data to the individual machines on the remote network.

> **NOTE:** To use the Java-based Network Explorer, you must have JRE installed on your local computer. JRE Version 1.6.0 Update 24 or newer is recommended. To download the latest Java and JRE versions, visit http://www.java.com. If the latest Java and JRE versions are not installed, an HTML-based Network Explorer is used, as explained in Using the HTML-Based Network Explorer

The administrator must enable Network Explorer for users to use it. To use the Java-based Network Explorer, click the **Java client** link on the top right section of the HTML-Based Network Explorer window.

The remote computer must have shared folders for files to be copied or moved. Sharing policy must be set from within the remote computer’s own operating system.

In Network Explorer, each pane has its own controls and displays a Location Bar, which shows the current path of each window. Entering a path in the Location Bar will take you to the specified location. Use backward slashes in the path for a Windows resource; otherwise, use forward slashes.



```
C:\Documents and Settings\sweigand\My Documents\SnagIt Catalog
Aventail_10.6.0_AgileUploaded.png
Aventail_10.6.0_firmware_md5_match.png
Aventail_10.6.0_ova_md5_match.png
ECM_monitor_disabled.png
faq_max_count_table16.png
HA_network_diagram.jpg
Image-0000.gif
Image-0000.png
Image-0001.gif
Image-0001.png
Image-0002.gif
Image-0002.png
Image-0003.png
Image-0004.gif
Image-0006.gif
Image-0007.gif
Image-0008.gif
Image-0009.gif
Image-0010.gif
Image-0011.gif
Image-0012.gif
Image-0013.gif
Image-0015.gif
Image-0019.gif
Image-0020.gif
Image-0021.gif
```

```
//10.4.2.45/Public/10.6.0-BETA1/
ex_sra_vm_10.6.0-034beta1.ova
ex_sra_vm_10.6.0-034beta1.ova.md5
upgrade-10.6.0-034beta1.bin
upgrade-10.6.0-034beta1.bin.md5
```

The remote pane may take some time to refresh, since the application needs to poll the EX-Series appliance for its contents. During such a procedure, the remote pane is grayed out and a **Cancel** button is displayed. Clicking the Cancel button will cancel the current operation and revert the remote pane to the previous location.

ⓘ **NOTE:** If the contents of the local or remote pane extend beyond the size of the window, a scroll bar will appear in the respective pane. You can scroll the window by using the scroll bar or mouse wheel.

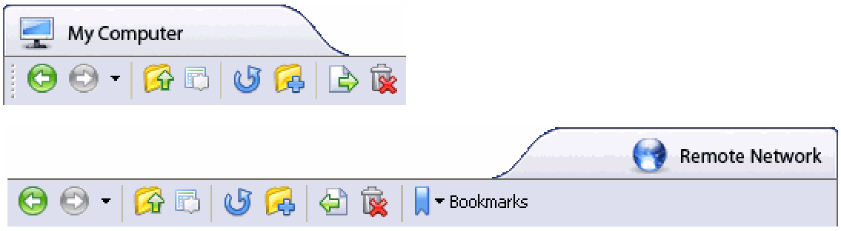
Object properties can be retrieved by right-clicking the item and selecting *Properties*. A window displaying the attributes of the object will appear.

- About the Network Explorer Toolbars
- Creating Bookmarks in Network Explorer
- Copying or Moving Files or Folders
- Opening or Launching a File in Network Explorer
- Deleting Files or Folders

About the Network Explorer Toolbars

Each pane has a toolbar with a set of icons for commonly used operations. Hovering the mouse cursor over these icons displays convenient tool tips to the user. Dragging the toolbar by the dotted line on the left side of it, or by an empty area at the right, undocks the toolbar into its own window. To re-dock the toolbar, simply close the window.

The toolbar for the remote pane includes the **Bookmarks** button, while the local pane does not. Bookmarks serve as useful shortcuts to quickly access different network locations. Users can create bookmarks by using the bookmark option on the right-click menu.



The buttons on the toolbar, from left to right, provide the following functions:

Back Traverses back in the history. Sets the current view of the window to the previous location in history. This icon is dimmed if there is no previous history location. Network Explorer maintains a 20-operation history for each pane.

Forward Traverses forward in history. This icon is dimmed if there are no forward locations in history.

Up Traverses up the directory tree to the parent directory of the current view. This icon is dimmed if the current view is of the root directory or if the parent directory cannot be resolved.

Sort Reverses the order of the listed files.

Refresh Refreshes the current view by either polling the local file system or remote network via the appliance. The refresh icon is dimmed in the remote window while its contents are being refreshed.

New Folder Creates a new folder within the respective file system. Clicking this icon will bring up the "New Folder" dialog box, allowing the user to assign a name to the new folder. This icon is dimmed when the location of the window is such that a new folder cannot be created. (eg. Root of a Windows file system, domain list, machine list)

Copy Copies the selected file(s)/folder(s) to the location of the remote window. Clicking this icon will bring up the "Copy" or "Move" dialog box that will show the status information of the copy procedure. If the file being copied already exists, a new dialog will show up asking the user whether or not the existing file should be replaced. The copy icon is dimmed when there are no selected files/folders to copy (eg. Nothing selected, drive or domain is selected). It is also dimmed if the remote location cannot accept files copied to it (eg. domain list, machine list).

Delete Deletes the selected files or folders.

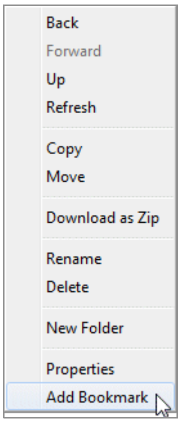
Bookmarks (Remote pane only) Displays the list of bookmarks. You can create bookmarks by using the bookmark option on the right-click menu.

Creating Bookmarks in Network Explorer

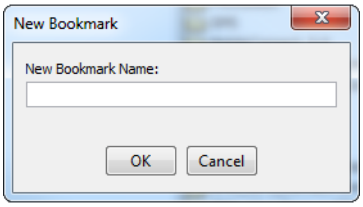
Bookmarks allow you to avoid lengthy navigations through a remote directory hierarchy, clicking one folder at a time. Creating a bookmark lets you bypass the hierarchy when accessing the target directory.

1 In the right pane of Network Explorer, navigate to the remote location for which you would like to create a bookmark.

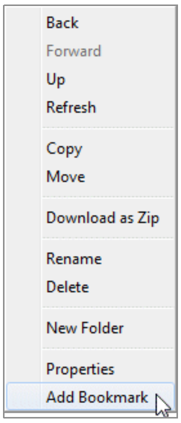
2 To set a bookmark to the current directory, right-click in an empty location in the remote directory and select **Add Bookmark** from the right-click menu.



3 Enter a name for the new bookmark in the **New Bookmark** window that displays, then click **OK**.



4 To set a bookmark for a specific file or folder, right-click the file or folder name and then select **Add Bookmark** from the right-click menu.



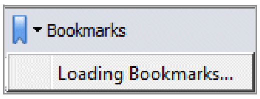
5 Enter a name for the new bookmark in the **New Bookmark** window that displays, then click **OK**.

Your bookmarks will also appear in the **Personal Bookmarks** area of the WorkPlace home page.

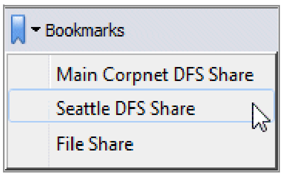
Using Bookmarks in Network Explorer

Once a bookmark is created, use it to bypass the remote directory hierarchy when accessing the target directory.

1 In Network Explorer, click on the **Bookmarks** button on the tool bar in the remote pane. A drop-down menu displays with the message *Loading Bookmarks*. Keep the mouse within the drop-down menu as Network Explorer loads the bookmarks.



2 Once the list is loaded, click the bookmark to access the desired file or folder.



Copying or Moving Files or Folders

For ease of use, there are several ways to perform file transfers using Network Explorer.

Moving or copying a directory or folder will move or copy all contents of the folder, including nested sub-directories. When a file or folder is moved, the item is deleted from the original location.

To copy or move files or folders:

1. In either the local or remote pane of Network Explorer, select the file or folder to be copied or moved.

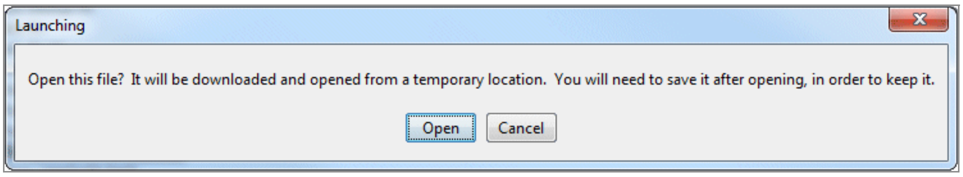
   To select multiple items, click the items while holding the Shift or the Ctrl key. Clicking on an item again while holding the Ctrl key will de-select it from the group.

2. To copy the item to the location displayed in the other pane, do one of the following:
   - Click-and-drag the item across the center boundary. You can also drop the item onto a folder name to copy it into that folder.
   - Click the **Copy** button on the toolbar in the pane with the selected item.
   - Right-click the item and select **Copy** from the right-click menu.
3. To move the item to the location displayed in the other pane, right-click the item and select **Move** from the right-click menu.
4. If user credentials are required to create or replace a file in the target directory, an authentication window is displayed. To begin the copy or move process, enter your credentials and click **OK**. If the item cannot be moved to the target location, the operation is disallowed.
5. Wait for the operation to complete. A progress bar displays the waiting time required to copy or move the files.

Opening or Launching a File in Network Explorer

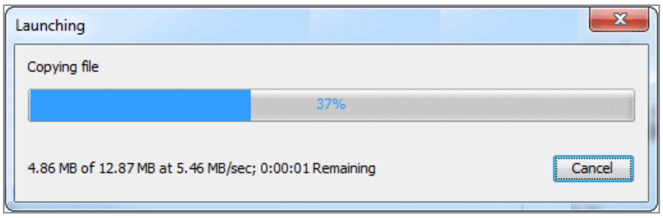
You can open files or launch applications on the remote filesystem in Network Explorer.

1. In Network Explorer, navigate to the location of the file in the remote pane.
2. Double-click on the desired file to launch it with the proper application.
3. If activating a file on the remote machine, Network Explorer will first download the file to a temporary folder on your local machine and then open it. In the Launching dialog box, click **Open** to proceed.



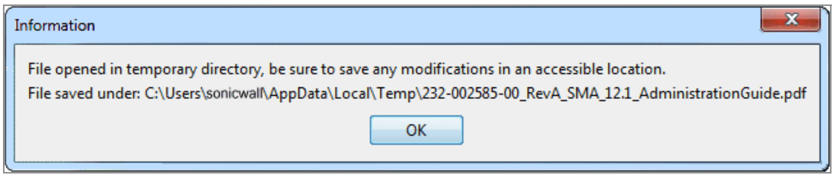
Open this file? It will be downloaded and opened from a temporary location. You will need to save it after opening, in order to keep it.

The progress of the download is displayed.



4.86 MB of 12.87 MB at 5.46 MB/sec; 0:00:01 Remaining

4 After the download completes, a message is displayed saying that you should save any changes to the file in an appropriate directory, as the file is opened in a temporary location. Click **OK** to proceed with opening or launching the file.



File opened in temporary directory, be sure to save any modifications in an accessible location.
File saved under: C:\Users\sonicwall\AppData\Local\Temp\232-002585-00_RevA_SMA_12.1_AdministrationGuide.pdf

Deleting Files or Folders

You can delete files or folders in Network Explorer.

1 In either the local or remote pane of Network Explorer, select the item you wish to delete.

To select multiple items, click the items while holding the Shift or the Ctrl key. Clicking on an item again while holding the Ctrl key will de-select it from the group.

2 Do one of the following to delete the item:

- Click the **Delete** button on the toolbar in the pane with the selected item.
- Right-click the item and select **Delete** from the right-click menu.

3 In the confirmation dialog box, click **Delete**.

Network Explorer will completely delete the file or folder from the remote machine. In the case of a folder, all files and folders under that resource will be recursively deleted. These items are not sent to the recycle bin on either machine and are not recoverable.

Using Secure Mobile Access Connect Agents

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

There is another application to launch that opens a specific Scheme URL. There are some Schemes already defined in the Windows/OS X, such as *mailto*. The Secure Mobile Access Connect Agent uses the Scheme URL to replace the Browser Plug-ins. The Secure Mobile Access Connect Agent is like a bridge that receives the Scheme URL requests and launches the specific native application.

To launch the Citrix Receiver through a Citrix bookmark, you must first install the Secure Mobile Access Connect Agent.

Topics:

- Supported Operating Systems
- Downloading and Installation
- Setting up the Secure Mobile Access Connect Agent

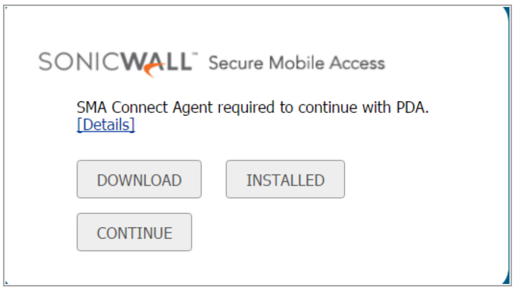
Supported Operating Systems

The Secure Mobile Access Connect Agent supports these operating systems:

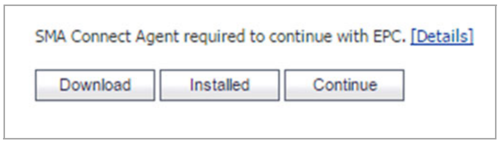
- Windows 7
- Windows 10
- Macintosh (OS X)

Downloading and Installation

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

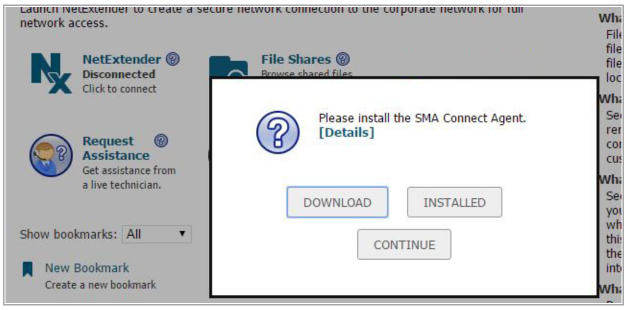


SMA Connect Agent required to continue with PDA.
[Details]



SMA Connect Agent required to continue with EPC. [Details]

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



Launch NetExtender to create a secure network connection to the corporate network for full network access.

Please install the SMA Connect Agent.
[Details]

- **Download** - Click Download to download and install Secure Mobile Access Connect Agent. After that, users can click Installed to tell the browser to 'remember' that the Secure Mobile Access Connect Agent has been installed, or click Continue just to bypass the page and log in to the StoreFront.
- **Installed** - the notification does not appear again.
- **Continue** - closes the notification and continues the action.
- **[Details]** - opens a window to introduce the Secure Mobile Access Connect Agent.

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

Setting up the Secure Mobile Access Connect Agent

Topics:

- Proxy Configuration
- Logs
- Browser Warning
- End Point Control (EPC)
- PDA (Personal Device Authorization)
- SonicWall Applications

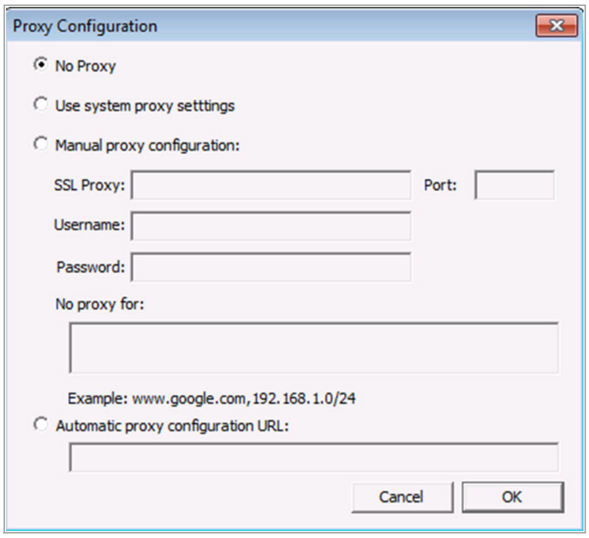
Proxy Configuration

Secure Mobile Access supports proxy deployment, where all client browsers are configured to redirect to a proxy server, but an appliance sits between the client browsers and the proxy server. All Secure Mobile Access features are supported in this scenario, including supporting domain exclusions when the domain is part of a virtual hosting server, or in some cloud deployments, wherein the same server IP can be used by multiple domains.

Additionally, typical data center server farms are fronted with a load balancer and/or reverse SSL Proxy to offload SSL processing on the servers. For a load balancer fronting the servers and doing decryption, the appliance usually only sees the IP of the load balancer, and the load balancer decrypts the content and determines the specific server to assign this connection to. DPI-SSL now has a global policy option to disable an IP-based exclusion cache. The exclusions continue to work even when the IP-based exclusion cache is off. The Secure Mobile Access Connect Agent can setup the proxy by user.

There are four options to setup the proxy configuration:

- **No Proxy** - When no proxy server is configured, IPv6 attributes are discarded.
- **Use system proxy settings**
- **Manual proxy configuration**
- **Automatic proxy configuration URL**



Proxy Configuration

● No Proxy

○ Use system proxy setttings

○ Manual proxy configuration:

SSL Proxy: Port:

Username:

Password:

No proxy for:

Example: www.google.com,192.168.1.0/24

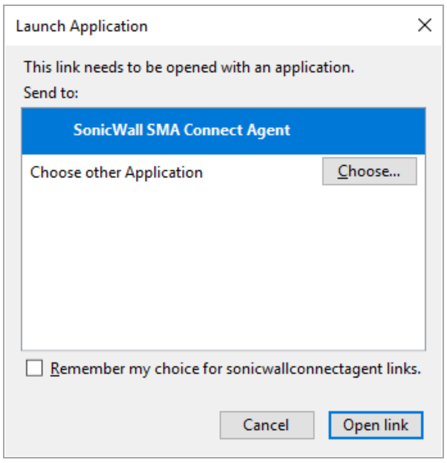
○ Automatic proxy configuration URL:

Logs

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

Browser Warning

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



Launch Application

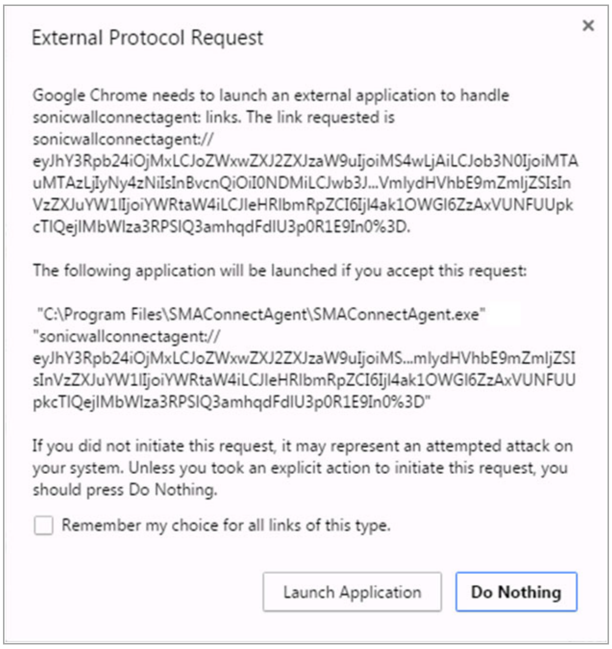
This link needs to be opened with an application.

Send to:

×
SonicWall SMA Connect Agent
Choose other Application
Choose...
□ Remember my choice for sonicwallconnectagent links.
Cancel
Open link

With a Fi*refox warning window, press* ***OK*** *to launch the Secure Mobile Access Connect Agent.*

*To launc*h the Citrix Native Bookmark, after logging in to the StoreFront, launch any Citrix desktops or applications such as other Citrix bookmarks. A browser confirmation message might appear.



External Protocol Request

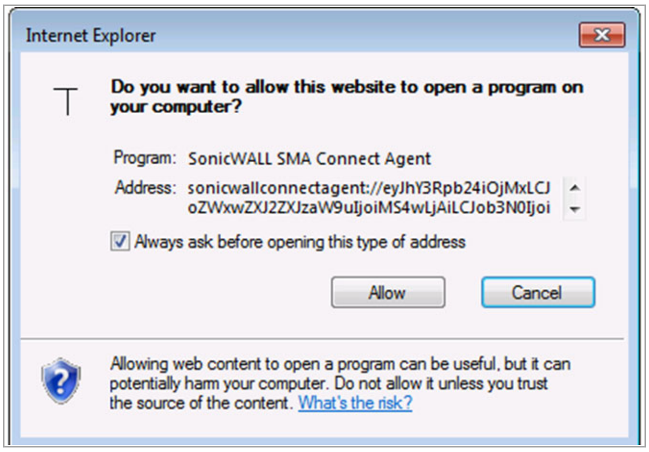
Google Chrome needs to launch an external application to handle sonicwallconnectagent: links. The link requested is sonicwallconnectagent://eyJhY3Rpb24iOjMxLCJoZWxwZXJ2ZXJzaW9uIjoiMS4wLjAiLCJob3N0IjoiMTAuMTAzLjIyNy4zNiIsInBvcnQiOiI0NDMiLCJwb3J...VmlydHVhbE9mZmljZSIsInVzZXJuYW1lIjoiYWRtaW4iLCJleHRlbmRpZCI6Ijl4ak1OWGI6ZzAxVUNFUUpkcTlQejlMbWlza3RPSlQ3amhqdFdlU3p0R1E9In0%3D.

The following application will be launched if you accept this request:

"C:\Program Files\SMAConnectAgent\SMAConnectAgent.exe" "sonicwallconnectagent://eyJhY3Rpb24iOjMxLCJoZWxwZXJ2ZXJzaW9uIjoiMS...mlydHVhbE9mZmljZSIsInVzZXJuYW1lIjoiYWRtaW4iLCJleHRlbmRpZCI6Ijl4ak1OWGI6ZzAxVUNFUUpkcTlQejlMbWlza3RPSlQ3amhqdFdlU3p0R1E9In0%3D"

If you did not initiate this request, it may represent an attempted attack on your system. Unless you took an explicit action to initiate this request, you should press Do Nothing.

In a Chrome warning window, press **Launch Application** to launch the Citrix or Secure Mobile Access Connect Agent.



Internet Explorer

Do you want to allow this website to open a program on your computer?

Program: SonicWALL SMA Connect Agent

Address: sonicwallconnectagent://eyJhY3Rpb24iOjMxLCJ oZWxwZXJ2ZXJzaW9uIjoiMS4wLjAiLCJob3N0Ijoi

☑ Always ask before opening this type of address

Allowing web content to open a program can be useful, but it can potentially harm your computer. Do not allow it unless you trust the source of the content. What's the risk?

In an Internet Explorer warning window, press Allow to launch the Secure Mobile Access Connect Agent.

End Point Control (EPC)

The Secure Mobile Access Connect Agent supports doing an EPC check from the browser. If you enable the EPC check in the login page, the browser launches the specific Scheme URL requesting the Secure Mobile Access Connect Agent do the EPC check.

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

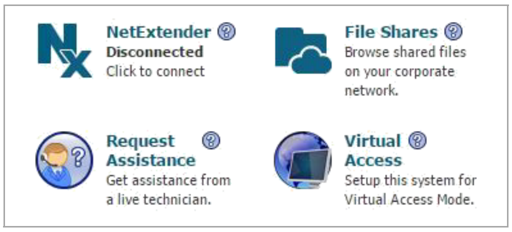
If the EPC feature (Appliance side) enables the “Show EPC failed message in detail at client side,” the Secure Mobile Access Connect Agent records the detailed fail message in the log. Then, you can view the tray Log.

PDA (Personal Device Authorization)

The PDA is a new feature. The Secure Mobile Access Connect Agent helps the PDA feature get the local machine's information. In the login page, if the user enables the PDA feature, the browser launches the Secure Mobile Access Connect Agent. Secure Mobile Access Connect gets the information of the local machine and sends the information to the appliance.

SonicWall Applications

On the portal page, there are buttons you can click to launch supported SonicWall Applications, including NetExtender, Virtual Assist, and Virtual Meeting.



NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Request Assistance
Get assistance from a live technician.
Virtual Access
Setup this system for Virtual Access Mode.

Cache Cleaner

Your system administrator can configure WorkPlace to require Cache Cleaner for data protection. Cache Cleaner provides data security by removing sensitive information from your computer after each session. This is especially important when you access your remote network from public computers, such as those found in Internet kiosks or hotel business centers.

Cache Cleaner performs cleanup actions and then exits when the following conditions occur:

- When you select **Logout** on the WorkPlace portal page
- When you close the browser window in which WorkPlace is running
- When you are inactive for a certain period of time (determined by your administrator)

Before it exits, Cache Cleaner removes all temporary data cached by any Web browser used during your network session, including cookies, browser history, stored passwords, auto-completion text, downloaded files, and temporary files.

Using Cache Cleaner

When enabled, Cache Cleaner automatically downloads and runs each time you log in to WorkPlace. Cache Cleaner will prompt you to accept a security warning that is displayed at WorkPlace startup.

Starting Cache Cleaner

During WorkPlace startup, in the security warning dialog box that appears, click **Continue**.

ⓘ **NOTE:** To prevent the security warning dialog box from appearing in the future, before clicking **Continue** expand **Show Options** and select the **Always trust connections to websites identified by this certificate** check box.

The Cache Cleaner icon appears in the taskbar notification area, and Cache Cleaner runs in the background during your network session.

If allowed by your administrator, you can disable Cache Cleaner. Once disabled, you can enable it again. If this option is not allowed, the **Disable** selection is grayed out in the right-click popup menu.

Disabling Cache Cleaner

Right-click the Cache Cleaner icon and select **Disable** in the popup menu.

Enabling Cache Cleaner

Right-click the Cache Cleaner icon and select **Enable** in the popup menu.

At the end of your network session, Cache Cleaner removes any temporary data stored on your system.

Exiting Cache Cleaner

Log out of WorkPlace. Upon logout, WorkPlace advises you that it will close all browser windows. A dialog box is displayed to notify you of this action and confirm your logout. To close all browser windows, click **OK**. To leave your browser windows open, click **Cancel**. If you select Cancel, your cached data will be deleted when all browser windows are closed.

Troubleshooting

This section describes how to troubleshoot basic connection problems.

Topics:

- Viewing Connection Status Information
- Viewing Security Zone Information
- Troubleshooting Tips

Viewing Connection Status Information

If you are having trouble accessing your network resources through WorkPlace, your system administrator may ask you for connection status information. You can view status information for any enabled access methods by clicking the **Details** link in the connection status area in WorkPlace. This displays the WorkPlace **System status** page, which includes information that can be helpful in troubleshooting connection problems.

Viewing Security Zone Information

Depending on how your administrator has configured WorkPlace, the **System status** page may display information about your current security zone. Your zone is determined by your environment or the type of computer you are using to access WorkPlace. For example, if you log in to WorkPlace from a laptop that your IT department owns and maintains, you may be placed in a more “trusted” zone than if you are logging in from an airport kiosk.

Your zone status may determine whether an SonicWall SMA data security agent (such as Cache Cleaner) is deployed. This zone information can also be helpful in troubleshooting WorkPlace problems.

Troubleshooting Tips

This section describes how to troubleshoot basic WorkPlace problems.

- Troubleshooting Full Network Access Problems
- Troubleshooting Agent Provisioning or Activation Problems

Troubleshooting Full Network Access Problems

If you are having trouble connecting to your network resources with full network access, see if your problem is addressed in the following list of troubleshooting tips. If the problem persists, contact your system administrator.

- If you use a personal firewall, you must configure the firewall before you can access your network resources. To do this, configure the firewall to allow *ngvpnmgr.exe* to access the Internet, and add the remote network’s host name or IP address as a trusted host or zone. For more information, contact your system administrator.
- Depending on how your administrator has configured WorkPlace, your local network resources may be unavailable when you are connected to the VPN. If you are unable to access a local network resource, such as a network printer, quit the access agent or log out of WorkPlace and then try again.

- If you are a restricted user (that is, without administrative privileges), ensure that your Web browser is configured to support Java. Note that you must be running the Java Runtime Environment (JRE); the Microsoft JVM is not supported.
- If you are an unrestricted user, ensure that your Web browser is configured to enable either ActiveX controls or Java.
- If you are prompted to enable the ActiveX control in your Web browser, be sure to click **Yes**.
- If you receive an error message indicating that the tunnel could not be established, contact your system administrator for more information.
- If you have full network access, you will see an icon in the taskbar notification area. If the access agent stops running or if you experience an interruption in service, a connection-status alert appears above this icon. The information displayed in this alert may be helpful in troubleshooting the problem.

Troubleshooting Agent Provisioning or Activation Problems

The first time you log in to WorkPlace, you may be prompted to install Secure Endpoint Manager. It installs and manages updates for any agents required to access your network. If an error occurs during the installation process, it is recorded in a log file that your system administrator can use to troubleshoot the problem. Once Secure Endpoint Manager is installed, the only other time you may be (briefly) aware of it is when an agent needs to be updated.

If you are having trouble installing or using an access agent, try the following:

- Enable ActiveX in your Web browser.
- Enable Java in your Web browser.
- Install the Java Runtime Environment (JRE) on your system.
- If you use a personal firewall, you may be prompted to block or permit access to Secure Endpoint Manager when you install it, or when you try to run an access agent. This dialog may pop up behind the WorkPlace browser window: if your login seems stalled, check to see if a security dialog is awaiting a response from you. If you are prompted, choose to permit access.
- Have your system administrator grant you the privileges required to install software on your computer.

After you have corrected the problem, click **Clear system profile** on the **System status** page to re-initialize your system, log out of WorkPlace, and then log in again.

In some cases, an access agent may not be activated due to a general connection error. If this occurs, log out of WorkPlace and then log in again.

2

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid 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://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

About This Document

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

Secure Mobile Access Workplace User Guide
Updated - May 2019
Software Version - 12.3
232-004854-00 Rev A

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 reserves 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.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035

3

SonicWall End User Product Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "***Agreement***") is made between you, the Customer ("**Customer**" or "**You**") and the Provider, as defined below.

1.**Definitions**. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a)"**Affiliate**" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b)"**Appliance**" means a computer hardware product upon which Software is pre-installed and delivered.

(c)"**Documentation**" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

(d) "**Maintenance Services**" means Provider's maintenance and support offering for the Products as identified in the Maintenance Services Section below.

(e)"**Partner**" means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

(f)"**Provider**" means, (i) for the US, Europe, Middle East, Africa, Latin America, and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Asia (other than Taiwan) SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland.

(g)"**Products**" means the Software and Appliance(s) provided to Customer under this Agreement.

(h)"**Software**" means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.

2.**Software License.**

(a)**General**. Subject to the terms of this Agreement, Provider grants to Customer, and Customer accepts from Provider, a non-exclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license to access and use the quantities of each item of Software purchased from Provider or a Partner within the parameters of the license type ("**License Type(s)**") described below in the quantities purchased ("License"). Except for MSP Licenses (as defined below), Customer shall only use the Software to support the internal business operations of itself and its worldwide Affiliates.

(b) **License Types.** The License Type for the Software initially delivered on the Appliance is "***per Appliance***". Software licensed per Appliance may be used only on the Appliance on which it is delivered, but without any other quantitative limitations. Software that is purchased on a subscription, or periodic basis is licensed by User or by Managed Node. A "**User**" is each person with a unique login identity to the Software. A "**Managed Node**" is any object managed by the Software including, but not limited to firewalls, devices, and other items sold by Provider.

(c)**Software as a Service.** When Customer purchases a right to access and use Software installed on equipment operated by Provider or its suppliers (the "***SaaS Software***"), (i) the License for such SaaS Software shall be granted for the duration of the term stated in the order (the "***SaaS Term***"), as such SaaS Term may be extended by automatic or agreed upon renewals, and (ii) the terms set forth in the SaaS Provisions Section of this Agreement shall apply to all access to and use of such Software. If any item of Software to be installed on Customer's equipment is provided in connection with SaaS Software, the License duration for such Software shall be for the corresponding SaaS Term, and Customer shall promptly install any updates to such Software as may be provided by Provider.

(d)**MSP License.**

"***Management Services***" include, without limitation, application, operating system, and database implementation, performance tuning, and maintenance services provided by Customer to its customers (each, a "***Client***") where Customer installs copies of the Software on its Clients' equipment or provides its Clients access to the Products. Customer shall be granted a License to use the Software and the associated Documentation to provide Management Services (the "***MSP License***"). Each MSP License is governed by the terms of this Agreement and any additional terms agreed to by the parties.

If the Product is to be used by Customer as a managed service provider, then Customer shall ensure that (i) Customer makes no representations or warranties related to the Products in excess of SonicWall's representations or warranties contained in this Agreement, (ii) each Client only uses the Products and Documentation as part of the Management Services provided to it by Customer, (iii) such use is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section of this Agreement, and (iv) each Client cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent. At the conclusion of any Management Services engagement with a Client, Customer shall promptly remove any Appliance and Software installed on its Client's computer equipment or require the Client to do the same. Customer agrees that it shall be jointly and severally liable to Provider for the acts and omissions of its Clients in connection with their use of the Software and Documentation and shall, at its expense, defend Provider against any action, suit, or claim brought against Provider by a Client in connection with or related to Customer's Management Services and pay any final judgments or settlements as well as Provider's expenses in connection with such action, suit, or claim.

(e)**Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an "***Evaluation License***"). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by Provider in writing (the "Evaluation Period"). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and capabilities which may not be available in SonicWall's generally available commercial versions of the Software. SonicWall retains the right during the term of the Evaluation License to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software.

NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED "AS IS", WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE BETA SOFTWARE'S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

(f)**Use by Third Parties.** Customer may allow its services vendors and contractors (each, a "**Third Party User**") to access and use the Products and Documentation provided to Customer hereunder solely for purposes of providing services to Customer, provided that Customer ensures that (i) the Third Party User's access to or use of the Products and Documentation is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section, (ii) the Third Party User cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent, and (iii) the Third Party Users promptly removes any Software installed on its computer equipment upon the completion of the Third Party's need to access or use the Products as permitted by this Section. Customer agrees that it shall be liable to Provider for those acts and omissions of its Third Party Users which, if done or not done by Customer, would be a breach of this Agreement.

3. **Restrictions**. Customer may not reverse engineer, decompile, disassemble, or attempt to discover or modify in any way the underlying source code of the Software, or any part thereof unless and to the extent (a) such restrictions are prohibited by applicable law and (b) Customer has requested interoperability information in writing from Provider and Provider has not provided such information in a timely manner. In addition, Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Products, Documentation or any part thereof, (ii) resell, sublicense or distribute the Products or Documentation, (iii) provide, make available to, or permit use of the Products, in whole or in part, by any third party (except as expressly set forth herein), (iv) use the Products or Documentation to create or enhance a competitive offering or for any other purpose which is competitive to Provider, (v) remove Software that was delivered on an Appliance from the Appliance on which it was delivered and load such Software onto a different appliance without Provider's prior written consent, or (vi) perform or fail to perform any other act which would result in a misappropriation or infringement of Provider's intellectual property rights in the Products or Documentation. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Notwithstanding anything otherwise set forth in this Agreement, the terms and restrictions set forth herein shall not prevent or restrict Customer from exercising additional or different rights to any open source software that may be contained in or provided with the Products in accordance with the applicable open source software licenses which shall be either included with the Products or made available to Customer upon request. Customer may not use any license keys or other license access devices not provided by Provider, including but not limited to "pirate keys", to install or access the Software.

4.**Proprietary Rights.** Customer understands and agrees that (i) the Products are protected by copyright and other intellectual property laws and treaties, (ii) Provider, its Affiliates and/or its licensors own the copyright, and other intellectual property rights in the Products, (iii) the Software is licensed, and not sold, (iv) this Agreement does not grant Customer any rights to Provider's trademarks or service marks, and (v) Provider reserves any and all rights, implied or otherwise, which are not expressly granted to Customer in this Agreement.

5. **Title.** Provider, its Affiliates and/or its licensors own the title to all Software.

6. **Payment.** Customer agrees to pay to Provider (or, if applicable, the Partner) the fees specified in each order, including any applicable shipping fees. Customer will be invoiced promptly following delivery of the Products or prior to the commencement of any Renewal Maintenance Period and Customer shall make all payments due to Provider in full within thirty (30) days from the date of each invoice or such other period (if any) stated in an order. Provider reserves the right to charge Customer a late penalty of 1.5% per month (or the maximum rate permitted by law, whichever is the lesser) for any amounts payable to Provider by Customer that are not subject to a good faith dispute and that remain unpaid after the due date until such amount is paid.

7.**Taxes.** The fees stated in an order from Provider or a Partner may not include taxes. If Provider is required to pay sales, use, property, value-added or other taxes based on the Products or Maintenance Services provided under this Agreement or on Customer's use of Products or Maintenance Services, then such taxes shall be billed to and paid by Customer. This Section does not apply to taxes based on Provider's or a Partner's income.

8. **Termination.**

(a)This Agreement or the Licenses granted hereunder may be terminated (i) by mutual written agreement of Provider and Customer or (ii) by either party for a breach of this Agreement by the other party (or a Third Party User) that the breaching party fails to cure to the non-breaching party's reasonable satisfaction within thirty (30) days following its receipt of notice of the breach. Notwithstanding the foregoing, in the case of MSP Licenses, if Customer or its Client breaches this Agreement two (2) times in any twelve (12) consecutive month period, the breaching party shall not have a cure period for such breach and Provider may terminate this Agreement immediately upon providing written notice to the breaching party.

(b)Upon termination of this Agreement or expiration or termination of a License for any reason, all rights granted to Customer for the applicable Software shall immediately cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) remove all copies, installations, and instances of the applicable Software from all Appliances, Customer computers and any other devices on which the Software was installed, and ensure that all applicable Third Party Users and Clients do the same, (iii) return the applicable Software to Provider together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iv) cease using the Maintenance Services associated with the applicable Software, (v) pay Provider or the applicable Partner all amounts due and payable up to the date of termination, and (vi) give Provider a written certification, within ten (10) days, that Customer, Third Party Users, and Clients, as applicable, have complied with all of the foregoing obligations.

(c)Any provision of this Agreement that requires or contemplates execution after (i) termination of this Agreement, (ii) a termination or expiration of a License, or (iii) the expiration of a SaaS Term, is enforceable against the other party and their respective successors and assignees notwithstanding such termination or expiration, including, without limitation, the Restrictions, Payment, Taxes, Termination, Survival, Warranty Disclaimer, Infringement Indemnity, Limitation of Liability, Confidential Information, Compliance Verification, and General Sections of this Agreement. Termination of this Agreement or a License shall be without prejudice to any other remedies that the terminating party or a Partner may have under law, subject to the limitations and exclusions set forth in this Agreement.

9. **Export.** Customer acknowledges that the Products and Maintenance Services are subject to the export control laws, rules, regulations, restrictions and national security controls of the United States and other applicable foreign agencies (the "Export Controls") and agrees to abide by the Export Controls. Customer hereby agrees to use the Products and Maintenance Services in accordance with the Export Controls, and shall not export, re-export, sell, lease or otherwise transfer the Products or any copy, portion or direct product of the foregoing in violation of the Export Controls. Customer is solely responsible for obtaining all necessary licenses or authorizations relating to the export, re-export, sale, lease or transfer of the Products and for ensuring compliance with the requirements of such licenses or authorizations. Customer hereby (i) represents that Customer, and if Customer is providing services under the MSP License herein each of its Clients, is not an entity or person to which shipment of Products, or provision of Maintenance Services, is prohibited by the Export Controls; and (ii) agrees that it shall not export, re-export or otherwise transfer the Products to (a) any country subject to a United States trade embargo, (b) a national or resident of any country subject to a United States trade embargo, (c) any person or entity to which shipment of Products is prohibited by the Export Controls, or (d) anyone who is engaged in activities related to the design, development, production, or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or chemical or biological weapons. Customer shall, at its expense, defend Provider and its Affiliates from any third party claim or action arising out of any inaccurate representation made by Customer regarding the existence of an export license, Customer's failure to provide information to Provider to obtain an export license, or any allegation made against Provider due to Customer's violation or alleged violation of the Export Controls (an "Export Claim") and shall pay any judgments or settlements reached in connection with the Export Claim as well as Provider's costs of responding to the Export Claim.

10. **Maintenance Services.**

(a) **Description.** During any Maintenance Period, Provider shall:

(i)Make available to Customer new versions and releases of the Software, if and when Provider makes them generally available without charge as part of Maintenance Services.

(ii)Respond to communications from Customer that report Software failures not previously reported to Provider by Customer. Nothing in the foregoing shall operate to limit or restrict follow up communication by Customer regarding Software failures.

(iii)Respond to requests from Customer's technical coordinators for assistance with the operational/technical aspects of the Software unrelated to a Software failure. Provider shall have the right to limit such responses if Provider reasonably determines that the volume of such non-error related requests for assistance is excessive or overly repetitive in nature.

(iv)Provide access to Provider's software support web site at https://support.sonicwall.com (the "***Support Site***").

(v) For Customers that have purchased Maintenance Services continuously since the purchase of such License, provide the repair and return program described on the Support Site for the Appliance on which the Software is delivered.

Maintenance Services are available during regional business support hours ("Business Hours") as indicated on the Support Site, unless Customer has purchased 24x7 Support. The list of Software for which 24x7 Support is available and/or required is listed in the Global Support Guide on the Support Site.

The Maintenance Services for Software that Provider has obtained through an acquisition or merger may, for a period of time following the effective date of the acquisition or merger, be governed by terms other than those in this Section. The applicable different terms, if any, shall be stated on the Support Site.

(b)**Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "Registration") and ends twelve (12) months thereafter (the "***Initial Maintenance Period***"). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a "***Renewal Maintenance Period***") For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a "***Maintenance Period.***" For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://support.sonicwall.com/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

For SaaS Software, the Maintenance Period is equal to the duration of the applicable SaaS Term. For non-perpetual Licenses or for non-perpetual MSP Licenses, the Maintenance Period is equal to the duration of the License.

11. **Warranties and Remedies.**

(a)**Software Warranties.** Provider warrants that, during the applicable Warranty Period (as defined in subsection (c) below),

(i) the operation of the Software, as provided by Provider, will substantially conform to its Documentation (the "***Operational Warranty***");

(ii) the Software, as provided by Provider, will not contain any viruses, worms, Trojan Horses, or other malicious or destructive code designed by Provider to allow unauthorized intrusion upon, disabling of, or erasure of the Software, except that the Software may contain a key limiting its use to the scope of the License granted, and license keys issued by Provider for temporary use are time-sensitive (the "***Virus Warranty***");

(iii)it will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of this Agreement by Customer that impacts the availability of the SaaS Software (the "***SaaS Availability Warranty***").

(b)**Appliance Warranties.** Provider warrants that, during the applicable Warranty Period, the Appliance will operate in a manner which allows the SNWL Software, respectively, to be used in substantial conformance with the Documentation (the ""***Appliance Warranty***",).

(c)**Warranty Periods.** The "***Warranty Period***" for each of the above warranties (except for E-class appliances which do not include a Software warranty, shall be as follows: (i) for the Operational Warranty as it applies to Software and the Virus Warranty, ninety (90) days following the initial Registration of the Software; (ii) for the Operational Warranty as it applies to SaaS Software and the SaaS Availability Warranty, the duration of the SaaS Term; and (iv) for the Appliance Warranty, one (1) year following the date the Appliance is registered with Provider.

(d)**Remedies.** Any breach of the foregoing warranties must be reported by Customer to Provider during the applicable Warranty Period. Customer's sole and exclusive remedy and Provider's sole obligation for any such breach shall be as follows:

(i)For a breach of the *Operational Warranty* that impacts the use of Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach within a reasonable time considering the severity of the error and its effect on Customer or, at Provider's option, refund the license fees paid for the nonconforming Software upon return of such Software to Provider and termination of the related License(s) hereunder.

(ii)For a breach of the *Operational Warranty* that impacts the use of SaaS Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach and provide a credit or refund of the fees allocable to the period during which the Software was not operating in substantial conformance with the applicable Documentation.

(iii)For a breach of the *Virus Warranty*, Provider shall replace the Software with a copy that is in conformance with the Virus Warranty.

(v)For a breach of the *SaaS Availability Warranty*, Provider shall provide a credit or refund of the fees allocable to the period during which the SaaS Software was not available for use.

(e)**Warranty Exclusions.** The warranties set forth in this Section shall not apply to any non-conformance (i) that Provider cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the applicable Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; or (iii) arising from the modification of the Product by anyone other than Provider.

(f)**Third Party Products.** Certain Software may contain features designed to interoperate with third-party products. If the third-party product is no longer made available by the applicable provider, Provider may discontinue the related product feature. Provider shall notify Customer of any such discontinuation, however Customer will not be entitled to any refund, credit or other compensation as a result of the discontinuation.

(g)**Warranty Disclaimer.** THE EXPRESS WARRANTIES AND REMEDIES SET FORTH IN THIS SECTION ARE THE ONLY WARRANTIES AND REMEDIES PROVIDED BY PROVIDER HEREUNDER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL OTHER WARRANTIES OR REMEDIES ARE EXCLUDED, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, AND ANY WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE. PROVIDER DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

(h)**High-Risk Disclaimer.** CUSTOMER UNDERSTANDS AND AGREES THAT THE PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HIGH-RISK OR HAZARDOUS ENVIRONMENT, INCLUDING WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION WHERE THE FAILURE OR MALFUNCTION OF ANY PRODUCT CAN REASONABLY BE EXPECTED TO RESULT IN DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR SEVERE ENVIRONMENTAL HARM (A "***HIGH RISK ENVIRONMENT***"). ACCORDINGLY, (I) CUSTOMER SHOULD NOT USE THE PRODUCTS IN A HIGH RISK ENVIRONMENT, (II) ANY USE OF THE PRODUCTS BY CUSTOMER IN A HIGH RISK ENVIRONMENT IS AT CUSTOMER'S OWN RISK, (III) PROVIDER, ITS AFFILIATES AND SUPPLIERS SHALL NOT BE LIABLE TO CUSTOMER IN ANY WAY FOR USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT, AND (IV) PROVIDER MAKES NO WARRANTIES OR ASSURANCES, EXPRESS OR IMPLIED, REGARDING USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT.

12.**Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a "***Claim***"). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a Claim or an injunction, Customer must stop using any Software ("***Infringing Software***"), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

13.**Limitation of Liability**. EXCEPT FOR (A) ANY BREACH OF THE *RESTRICTIONS* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, (B) AMOUNTS CONTAINED IN JUDGMENTS OR SETTLEMENTS WHICH PROVIDER OR CUSTOMER IS LIABLE TO PAY TO A THIRD PARTY UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER IS LIABLE TO PAY ON BEHALF OF OR TO PROVIDER UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES SECTIONS* OF THIS AGREEMENT, OR (C) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, IN NO EVENT SHALL CUSTOMER OR ITS AFFILIATES, OR PROVIDER, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR (X) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND OR (Y) LOSS OF REVENUE, LOSS OF ACTUAL OR ANTICIPATED PROFITS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF GOODWILL OR REPUTATION, LOSS OF ANTICIPATED SAVINGS, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA, HOWSOEVER ARISING, WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR IN THE CONTEMPLATION OF THE PARTIES AND WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE.

EXCEPT FOR (A) ANY BREACH OF THE *SOFTWARE LICENSE*, *RESTRICTIONS*, OR CONFIDENTIAL INFORMATION SECTIONS OF THIS AGREEMENT, OR ANY OTHER VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) PROVIDER'S EXPRESS OBLIGATIONS UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER'S EXPRESS OBLIGATIONS UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, (C) PROVIDER'S COSTS OF COLLECTING DELINQUENT AMOUNTS WHICH ARE NOT THE SUBJECT OF A GOOD FAITH DISPUTE; (D) A PREVAILING PARTY'S LEGAL FEES PURSUANT TO THE *LEGAL FEES* SECTION OF THIS AGREEMENT; OR (E) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY OF CUSTOMER AND ITS AFFILIATES, AND PROVIDER, ITS AFFILIATES AND SUPPLIERS, FOR DAMAGES UNDER THIS AGREEMENT, WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE, SHALL BE AN AMOUNT EQUAL TO (Y) THE GREATER OF THE FEES PAID AND/OR OWED (AS APPLICABLE) BY CUSTOMER OR ITS AFFILIATES FOR THE PRODUCTS THAT ARE THE SUBJECT OF THE BREACH OR FIVE HUNDRED DOLLARS ($500.00),EXCEPT FOR (Z) MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, FOR WHICH THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY SHALL BE THE GREATER OF THE AMOUNT PAID AND/OR OWED (AS APPLICABLE) FOR SUCH MAINTENANCE SERVICE OR PRODUCT DURING THE TWELVE (12) MONTHS PRECEDING THE BREACH OR FIVE HUNDRED DOLLARS ($500.00). THE PARTIES AGREE THAT THESE LIMITATIONS OF LIABILITY ARE AGREED ALLOCATIONS OF RISK CONSTITUTING IN PART THE CONSIDERATION FOR PROVIDER PROVIDING PRODUCTS AND SERVICES TO CUSTOMER, AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES OR FAILURES.

Provider's Affiliates and suppliers and Customer's Affiliates shall be beneficiaries of this Limitation of Liability Section and Customer's Clients and Third Party Users are entitled to the rights granted under the MSP License and Use by Third Parties Sections of this Agreement; otherwise, no third party beneficiaries exist under this Agreement. Provider expressly excludes any and all liability to Third Party Users, Clients and to any other third party.

14.**Confidential Information.**

(a)**Definition.** "***Confidential Information***" means information or materials disclosed by one party (the "***Disclosing Party***") to the other party (the "***Receiving Party***") that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential, including, without limitation, financial, marketing, and pricing information, trade secrets, know-how, proprietary tools, knowledge and methodologies, the Software (in source code and/or object code form), information or benchmark test results regarding the functionality and performance of the Software, any Software license keys provided to Customer, and the terms and conditions of this Agreement.

Confidential Information shall not include information or materials that (i) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the date that Customer accepts the Agreement (the "***Effective Date***"); (ii) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (iii) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; (iv) are protected by Provider in accordance with its obligations under the Protected Data Section below, or (v) are or were independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

(b)**Obligations.** The Receiving Party shall (i) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (c) below and (ii) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care. The Receiving Party shall promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information and will cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights. For the avoidance of doubt, this Section shall apply to all disclosures of the parties' Confidential Information as of the Effective Date, whether or not specifically arising from a party's performance under this Agreement.

(c)**Permitted Disclosures.** Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent to any of its Affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the "***Representatives***"), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this Agreement or to provide professional advice in connection with this Agreement, (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein, and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential Information and the requirements regarding restrictions on disclosure and use as set forth in this Section. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this Agreement.

Additionally, it shall not be a breach of this Section for the Receiving Party to disclose the Disclosing Party's Confidential Information as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction.

15.**Protected Data.** For purposes of this Section, "***Protected Data***" means any information or data that is provided by Customer to Provider during this Agreement that alone or together with any other information relates to an identified or identifiable natural person or data considered to be personal data as defined under Privacy Laws, and "***Privacy Laws***" means any applicable law, statute, directive or regulation regarding privacy, data protection, information security obligations and/or the processing of Protected Data.

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or access to Protected Data by third parties, and shall only store and process Protected Data as may be required to fulfill its obligations under this Agreement. If Provider complies with Customer's written instructions with respect to the Protected Data, Provider shall have no liability to Customer for any breach of this Section resulting from such compliance. Provider shall promptly notify Customer of any disclosure of or access to the Protected Data by a third party in breach of this Section and shall cooperate with Customer to reasonably remediate the effects of such disclosure or access. Provider further affirms to Customer that it has adequate agreements in place incorporating the EU standard contractual clauses for the transfer of Protected Data from the European Union ("EU") to a country outside the EU.

Customer hereby (i) represents that it has the right to send the Protected Data to Provider, (ii) consents for Provider to store and use the Protected Data worldwide for the sole purpose of performing its obligations under this Agreement, (iii) agrees that the Protected Data may be accessed and used by Provider and its Representatives worldwide as may be needed to support Provider's standard business operations, and (iv) agrees that Protected Data consisting of Customer contact information (e.g., email addresses, names) provided as part of Maintenance Services may be sent to Provider's third party service providers as part of Provider's services improvement processes.

16**.Compliance Verification.** Customer agrees to maintain and use systems and procedures to accurately track, document, and report its installations, acquisitions and usage of the Software. Such systems and procedures shall be sufficient to determine if Customer's deployment of the Software or, if applicable, use of the SaaS Software is within the quantities, terms, and maintenance releases to which it is entitled. Provider or its designated auditing agent shall have the right to audit Customer's deployment of the Software or, if applicable, use of the SaaS Software for compliance with the terms and conditions of this Agreement. Any such audits shall be scheduled at least ten (10) days in advance and shall be conducted during normal business hours at Customer's facilities. Customer shall provide its full cooperation and assistance with such audit and provide access to the applicable records and computers. Without limiting the generality of the foregoing, as part of the audit, Provider may request, and Customer agrees to provide, a written report, signed by an authorized representative, listing Customer's then current deployment of the Software and/or the number of individuals that have accessed and used SaaS Software. If Customer's deployment of the Software or, if applicable, use of the SaaS Software is found to be greater than its purchased entitlement to such Software, Customer will be invoiced for the over-deployed quantities at Provider's then current list price plus the applicable Maintenance Services and applicable over-deployment fees. All such amounts shall be payable in accordance with this Agreement. Additionally, if the unpaid fees exceed five percent (5%) of the fees paid for the applicable Software, then Customer shall also pay Provider's reasonable costs of conducting the audit. The requirements of this Section shall survive for two (2) years following the termination of the last License governed by this Agreement.

17.**SaaS Provisions.**

(a)**Data.** Customer may store data on the systems to which it is provided access in connection with its use of the SaaS Software (the "***SaaS Environment***"). Provider may periodically make back-up copies of Customer data, however, such back-ups are not intended to replace Customer's obligation to maintain regular data backups or redundant data archives. Customer is solely responsible for collecting, inputting and updating all Customer data stored in the SaaS Environment, and for ensuring that it does not (i) knowingly create and store data that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party, or (ii) use the SaaS Environment for purposes that would reasonably be seen as obscene, defamatory, harassing, offensive or malicious. Provider shall have the right to delete all Customer data stored in connection with the use of the SaaS Software thirty (30) days following any termination of this Agreement or any License to SaaS Software granted hereunder.

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

(b)**Conduct.** In connection with the use of SaaS Software, Customer may not (i) attempt to use or gain unauthorized access to Provider's or to any third-party's networks or equipment; (ii) permit other individuals or entities to copy the SaaS Software; (iii) provide unauthorized access to or use of any SaaS Software or the associated access credentials; (iv) attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (v) interfere or attempt to interfere with service to any user, host or network; (vi) engage in fraudulent, offensive or illegal activity of any nature or intentionally engage in any activity that infringes the intellectual property rights or privacy rights of any individual or third party; (vii) transmit unsolicited bulk or commercial messages; (viii) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items; (ix) restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the SaaS Software (except for tools with safety and security functions); or (x) restrict, inhibit, interfere with or otherwise disrupt or cause a performance degradation to any Provider (or Provider supplier) facilities used to provide the SaaS Environment. Customer shall cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a "***Third Party Claim***") alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

(c)**Suspension.** Provider may suspend Customer's use of SaaS Software (a) if so required by law enforcement or legal process, (b) in the event of an imminent security risk to Provider or its customers, or (c) if continued use would subject Provider to material liability. Provider shall make commercially reasonable efforts under the circumstances to provide prior notice to Customer of any such suspension.

18.**General.**

(a)**Governing Law and Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the Santa Clara County, California. Each party hereby agrees to submit to the jurisdiction of such courts. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated.

(b)**Assignment.** Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement, the Licenses granted under this Agreement or any other rights, interest or obligations hereunder, whether voluntarily, by contract, by operation of law or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Provider. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void.

(c)**Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible by law to effect the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Notwithstanding the foregoing, the terms of this Agreement that limit, disclaim, or exclude warranties, remedies or damages are intended by the parties to be independent and remain in effect despite the failure or unenforceability of an agreed remedy. The parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

(d)**Use by U.S. Government.** The Software is a "commercial item" under FAR 12.201. Consistent with FAR section 12.212 and DFARS section 227.7202, any use, modification, reproduction, release, performance, display, disclosure or distribution of the Software or Documentation by the U.S. government is prohibited except as expressly permitted by the terms of this Agreement. In addition, when Customer is a U.S. government entity, the language in Subsection (ii) of the *Infringement Indemnity* Section of this Agreement and the *Injunctive Relief* Section of this Agreement shall not be applicable.

(e)**Notices.** All notices provided hereunder shall be in writing and may be delivered by email, in the case of Provider to *legal@sonicwall.com* and in the case of Customer to the email address Provider has on file for Customer. All notices, requests, demands or communications shall be deemed effective upon delivery in accordance with this paragraph.

(f)**Disclosure of Customer Status.** Provider may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of Provider in its marketing communications.

(g)**Waiver.** Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

(h)**Injunctive Relief.** Each party acknowledges and agrees that in the event of a material breach of this Agreement, including but not limited to a breach of the *Software License*, *Restrictions* or *Confidential Information* Sections of this Agreement, the non-breaching party shall be entitled to seek immediate injunctive relief, without limiting its other rights and remedies.

(i**)Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures. For added certainty, this Section shall not operate to change, delete, or modify any of the parties' obligations under this Agreement (e.g., payment), but rather only to excuse a delay in the performance of such obligations.

(j)**Equal Opportunity.** Provider is a federal contractor and Affirmative Action employer (M/F/D/V) as required by the Equal Opportunity clause C.F.R. § 60-741.5(a).

(k)**Headings**. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

(l) **Legal Fees.** If any legal action is brought to enforce any rights or obligations under this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees, court costs and other collection expenses, in addition to any other relief it may be awarded.

(m)**Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed, non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.