



Secure Mobile Access 12.4

Workplace User Guide

SONICWALL®

Contents

Using Secure Mobile Access WorkPlace	3
WorkPlace Overview	3
WorkPlace Lite	4
Access Methods and Resources	5
Managing App based One-Time Password	6
Logging into WorkPlace	8
Changing Your Password	10
Entering Credentials Using the Virtual Keyboard	12
Logging out of WorkPlace	13
The Network Explorer Page	14
Accessing Network Resources	14
Using Shortcuts	15
Using the Intranet Address Box	17
Using Bookmarks	19
Options Using HTML	25
Overview	25
RDP Using HTML	26
Working with Folders and Files	27
Using the Network Explorer	27
Secure Endpoint Manager (SEM)	35
Unified Web Agent for Workplace or browser access	35
Supported Operating Systems and Browsers	35
Installing Secure Endpoint Manager	36
Setting up the Secure Mobile Access Connect Agent	39
Troubleshooting	45
Viewing Connection Status Information	45
Viewing Security Zone Information	45
Troubleshooting Tips	46
SonicWall Support	47
About This Document	48

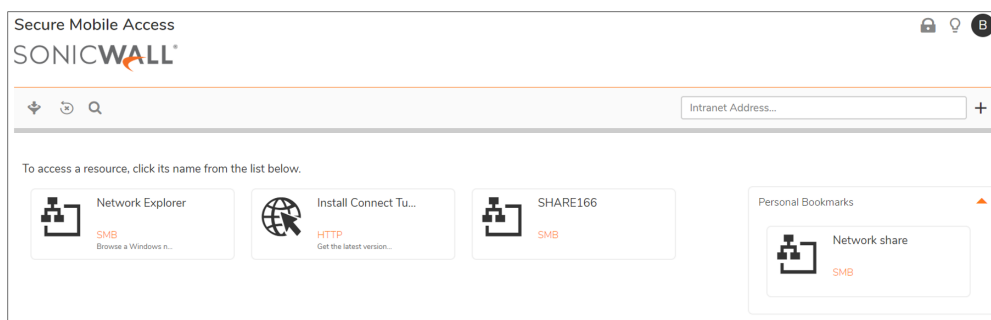
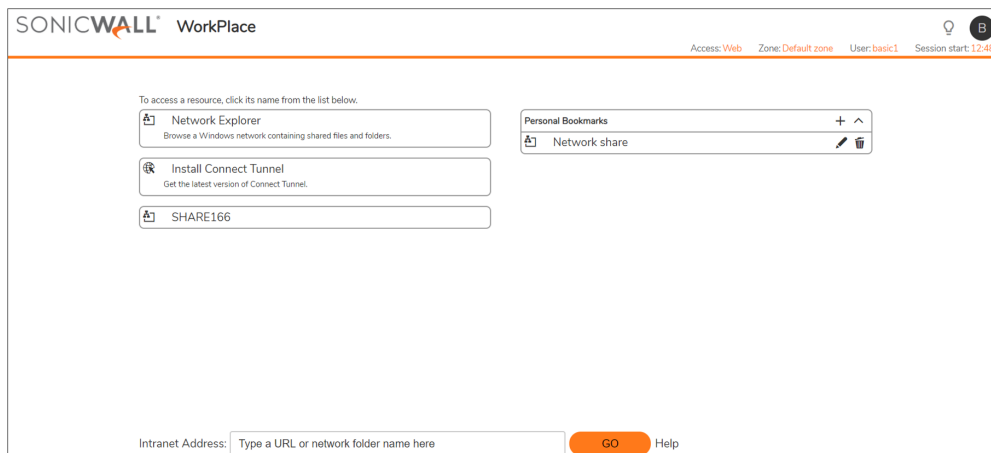
Using Secure Mobile Access WorkPlace

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](#)
- [WorkPlace Lite](#)
- [Access Methods and Resources](#)
- [Logging into WorkPlace](#)
- [Logging out of WorkPlace](#)
- [Accessing Network Resources](#)
- [Options Using HTML](#)
- [Using Bookmarks](#)
- [Working with Folders and Files](#)
- [Secure Endpoint Manager \(SEM\)](#)
- [Using the Network Explorer](#)
- [Troubleshooting](#)


WorkPlace Overview

When you access the 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.



The Workplace home page includes connection status information indicating which access methods are currently enabled and the session start time. You can click the **Logged In User > Details** 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 . 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.

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 is a modern web browser that supports HTML. 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 the checkbox for Lite access in the Log in page. 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.

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.

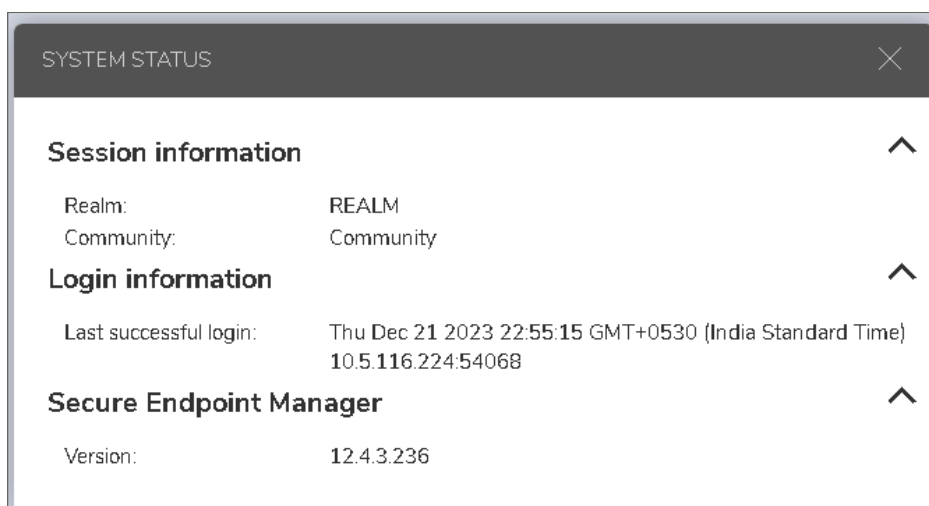
ACCESS METHODS AND RESOURCES

Access method	Resources available
Web	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 **Logged In User > Details**, which provides access to the following features:

- Session information - Identifies the Zone, Realm, and Community.
- Login Information - Provides the login time stamp along with system IP details. Device Authorization Terms - Provides an Authorization Terms and consent form to allow access to the network resources from a personal device.
- Secure Endpoint Manager - Identifies the version of Secure Endpoint Manager 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).



For more information on App based one-time password, refer to [Managing App based One-Time Password](#).

Managing App based One-Time Password

You can manage your app based one-time password account from Workplace if allowed by admin. From Workplace, you can register a new device for app based one-time password in situations when you need to switch to a new mobile device. You can also view your current list of backup codes and renew them.

To manage app based one-time passwords:

1. Click **Logged In User > Details**.
The **System Status** is displayed.
The available list of **Backup codes** are displayed under **App based One-Time Password** to log into the Workplace portal when needed.

SYSTEM STATUS

Session information

Zone:

Default zone

Realm:

LocalDB

Community:

Local_comm

Data protection:

None

WorkPlace Lite:

Enabled

Login information

There have been 4 failed login attempts since your last successful authentication.

Last successful login:

Thu Jul 14 2022 14:33:09

GMT+0530 (India Standard Time)

10.65.20.80:59278

Last failed login:

Mon Jul 18 2022 15:16:14

GMT+0530 (India Standard Time)

10.65.20.185:54296

App based One-Time Password

Backup codes:

7J6HMH5, 6GAC5CWJ,

PJVVS50, 25WKULNL,

ZZ2HF4E2

Renew

Deregister

- In order to generate a new set of codes, in situations where you think your current codes are compromised, click **Renew** to generate new set of backup codes.

NOTE: Each code can be used only once. If you have exhausted the codes, then click **Renew** to regenerate new backup codes.
- To register a new mobile device, click **Deregister** to remove the App based One-Time Password account from appliance.

Once unregistered, you can remove the account from mobile device. You are prompted to register during next log in.

SMA 12.4 Workplace User Guide
Using Secure Mobile Access WorkPlace

7

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.

① | **NOTE:** Keyboard entry may not be accepted when using RDP in full screen mode on macOS 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 **Refresh** icon.

SONICWALL[®]
WORKPLACE


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

Log in to:
Captcha

Username:

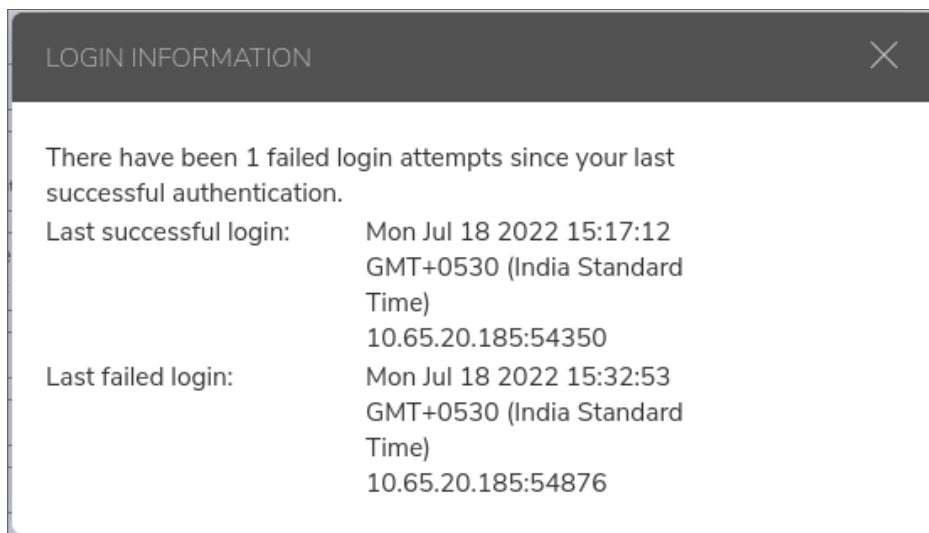
Password:

Help us make sure you are not a malicious program.
Type the verification text you see below.

0575 

Log in

7. You 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.
 - Your administrator can configure the SEM to start automatically when the operating system starts (Windows only).
8. Click **Log in**.
 - ① **NOTE:** If you try to log in with invalid credentials, the **Login Information** dialog box is displayed with the failed login attempts notification.



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 an user-initiated password change is allowed, you will see the **Change password** checkbox.

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

Username:

Password:

☐ Use virtual keyboard 

☐ Change password 

Log in

To change your password:

1. In the Log in screen, enter your current credentials.
2. Click **Change password**, and then click **Log in**.

The image shows a dark-themed dialog box for changing a password. At the top left is the 'SONICWALL' logo with 'WORKPLACE' underneath. Below the logo, the text 'Type your old password and specify your new password' is displayed. There are three input fields: 'Old password:' (with a dashed orange border), 'New password:' (with a solid orange border), and 'Verify new password:' (with a solid orange border). Below these fields is a checkbox labeled 'Use virtual keyboard' with a small keyboard icon. At the bottom are two buttons: 'OK' (orange) and 'Cancel' (white with an orange border). The right side of the dialog box features a curved orange border and a background image of clouds.

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

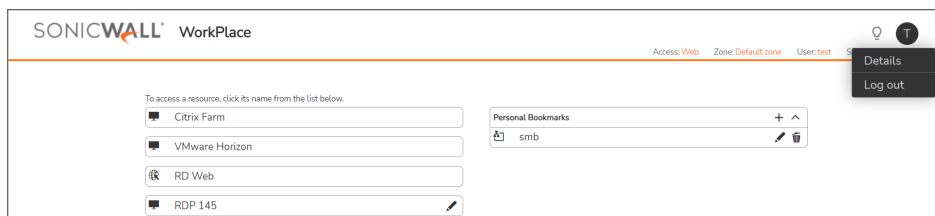
Log in

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 **Logged In User > Log out** 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.

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.

In the 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.

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.

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: GO [Help](#)

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:

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

To create a custom shortcut, see [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 shared folders or files open in a separate Network Explorer window. Clicking a Citrix and VMware server farm shortcut displays a window identifying its applications and desktops.

To Configure Custom Links

Click the **Edit** icon for the resource shortcut to open the **Edit 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**.

EDIT SHORTCUT

Adjust custom settings for the shortcut. Contact your system administrator for assistance.

Name:*

Address:*

Description:

Shortcut type:

Client type:

Screen resolution:

Color depth:

Connection type:

Keyboard layout:

☐ Connect to admin/console session

☒ Display connection bar

☐ Enable multi-monitor support

☒ Remote audio playback

☐ Remote audio recording

☐ Redirect Cameras

☐ Redirect SmartCards

☐ Enable third-party plugin DLLs

☐ Enable Wake-on-LAN (WoL)

☐ Enable Single Sign-On

☐ Use Mobile Connect Secure Web Browser

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, web resources, and terminal servers.

Intranet Address:

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.

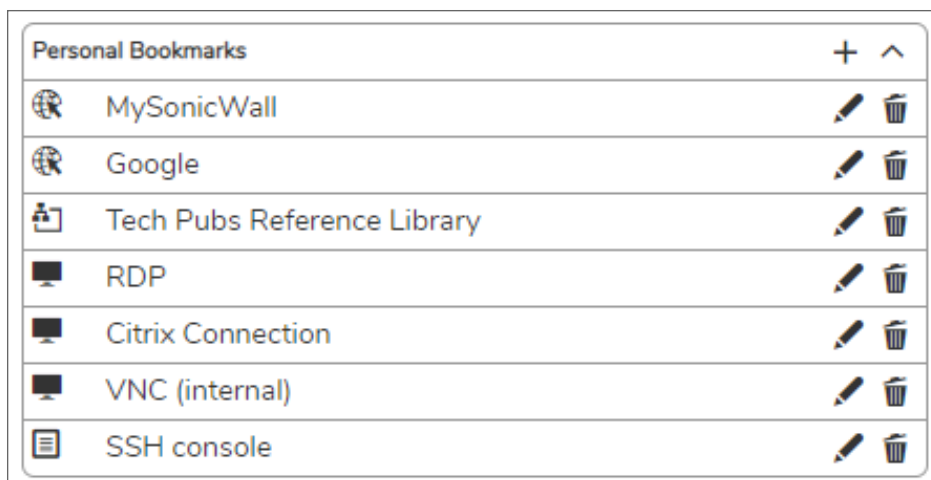
When specifying a terminal server resource URL, you must include the appropriate protocol identifier. If a terminal server resource contains multiple hosts, you are prompted to type the host name or IP address of the specific resource you want to access.

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

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.



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.

Topics:


- [Adding Bookmarks](#)
- [Reordering Bookmarks](#)
- [Editing Bookmarks](#)
- [Deleting Bookmarks](#)

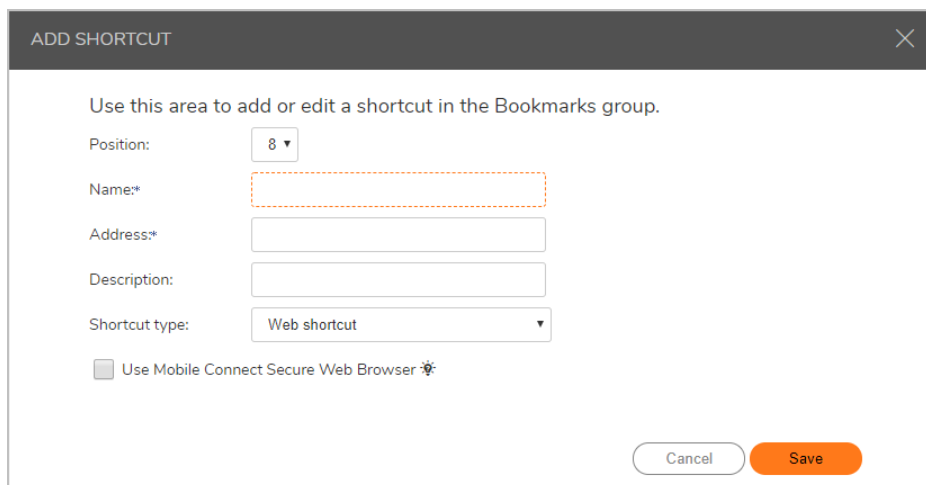
Adding Bookmarks

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.

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

To add a bookmark:

1. In the **Personal Bookmarks** group in WorkPlace, click .
The **Add Shortcut** page appears.



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:

The screenshot shows a dialog box titled "ADD SHORTCUT" with a close button (X) in the top right corner. Inside the dialog, there is a text instruction: "Use this area to add or edit a shortcut in the Bookmarks group." Below this, there are several input fields and a dropdown menu:

- Position:** A dropdown menu showing "4".
- Name:*** A text input field containing "MySonicWall".
- Address:*** A text input field containing "https://mysonicwall.com".
- Description:** A text input field containing "MySonicWall Home Page".
- Shortcut type:** A dropdown menu with "Web shortcut" selected and highlighted in blue. The dropdown list also includes "Network shortcut", "RDP shortcut", "Citrix shortcut", "VNC shortcut", "SSH shortcut", and "Telnet shortcut".
- Use Mobile Connection:** A checkbox that is currently unchecked.

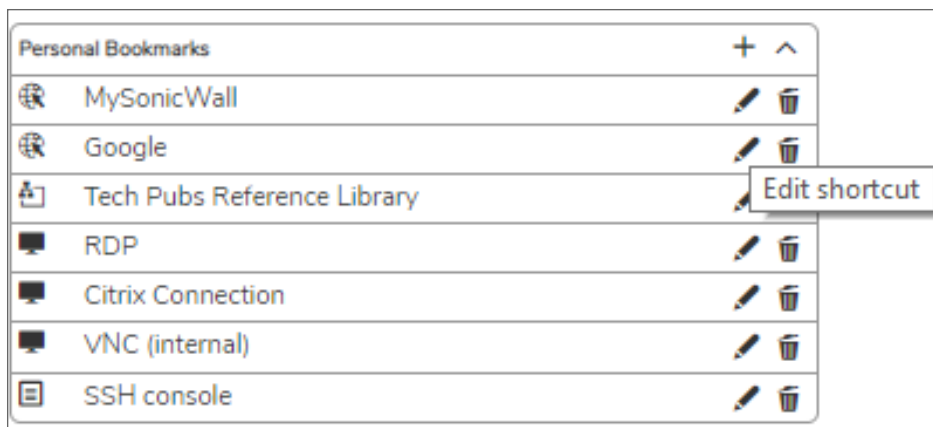
At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

An RDP shortcut might be configured as shown below:


7. Click **Save**.

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

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



To reorder the bookmarks:

1. In the **Personal Bookmarks** group in WorkPlace, click  on the bookmark which you want to reorder. The **Edit Shortcut** dialog appears.

EDIT SHORTCUT

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

Position: 1 ▼

Name: 1 nicWall

Address: 2 /mysonicwall.com/

Description: 3

Shortcut type: 4 shortcut ▼

☐ Use Mobile Connection 5 re Web Browser

6

7


Cancel Save

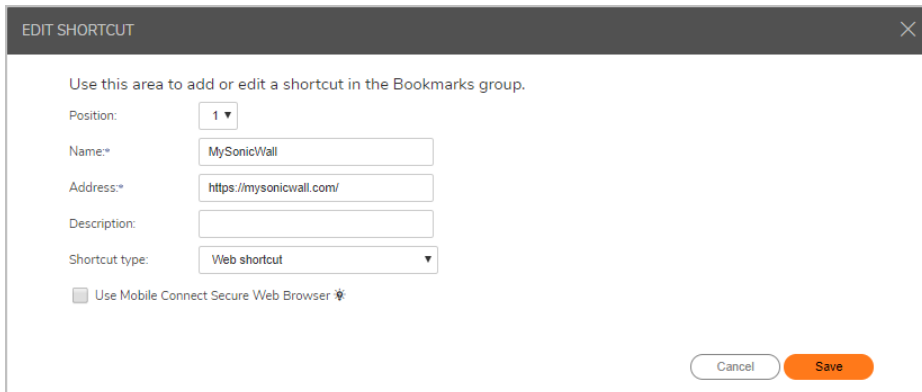
2. Select the desired position for the bookmark from the **Position** drop-down list.
3. Click **Save**.

Editing Bookmarks

You can edit the bookmarks after you have added them.

To edit a bookmark:

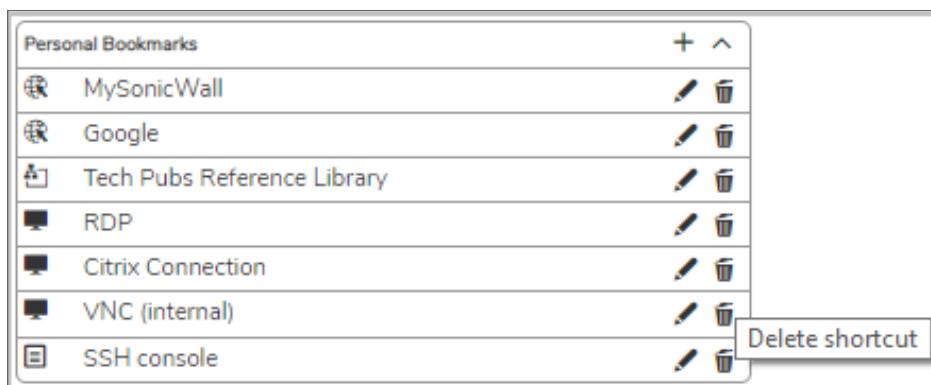
1. In the **Personal Bookmarks** group in WorkPlace, click  on the bookmark which you want to edit. The **Edit Shortcut** dialog displays.




2. Edit the values that you want to change.
3. Click **Save**.

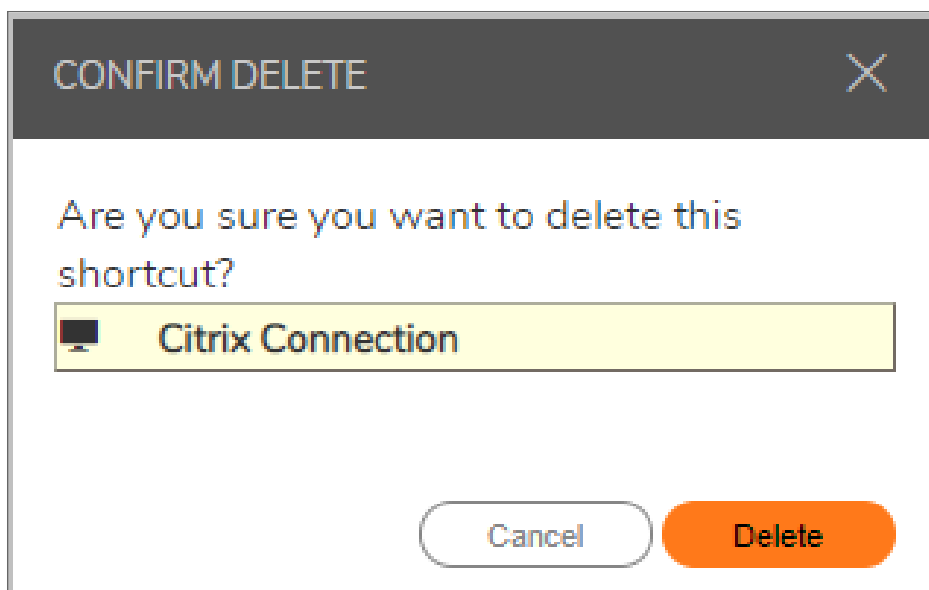
Deleting Bookmarks

You can delete bookmarks that you no longer need.



To delete a bookmark:

1. In the **Personal Bookmarks** group in WorkPlace, click  on the bookmark which you want to edit.
The **Confirm Delete** dialog appears.



2. Click **Delete**.

Options Using HTML

Topics:

- [Overview](#)
- [RDP Using HTML](#)

Overview

HTML clients can connect to backend systems using RDP, VNC, SSH, and Telnet. HTML 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.

① **NOTE:** RDP, VNC, SSH, and Telnet using HTML can be configured in SMA 12.4.3 onwards on an SMA 1000 series appliance or in SMA 12.4.3 WorkPlace onwards.

HTML clients eliminate the management of the endpoint clients, such as Java and ActiveX. The following table shows the HTML 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 HTML

Topics:

- [Keyboard Support for RDP](#)
- [Copy and Paste in HTML RDP](#)

① | **NOTE:** Server authentication for RDP is configured by the system administrator.

① | **NOTE:** Audio and Video recording for RDP shortcuts and bookmarks is supported from 12.4.3 version onwards.

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 from 12.4.3 onwards:

Bosnian	Greek
Bulgarian	Hungarian
Croatian	Irish
Czech	Italian
Danish	Lithuanian

Dutch	Luxembourgish
English (United Kingdom)	Norwegian
English (United States)	Polish
English (US - International)	Portuguese
Finnish	Romanian
French (Belgium)	Russian
French (Canada)	Spanish
French (France)	Swedish
French (Switzerland)	Turkish F, Turkish Q
German (Germany)	German (Switzerland)

Copy and Paste in HTML RDP

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

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

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.

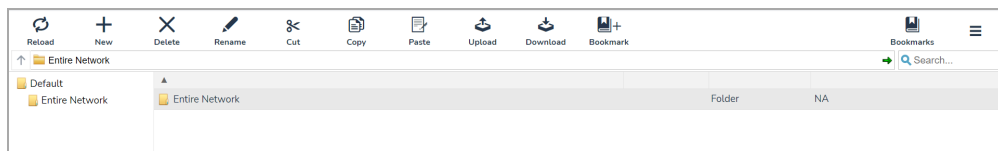
WorkPlace automatically displays the Network Explorer.

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. In the 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.

Using the Network Explorer

The 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 enter them.



The below table 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 files or folders. You will be prompted for confirmation before the folders are deleted.
Rename	Allows you to rename a selected folder or file.
Cut	Allows you to cut a selected folder or file.
Copy	Allows you to copy a selected folder or file.
Paste	Allows you to paste the copied or cut files and folders
Upload	Uploads the selected files or folders to the selected network folder.
Download	Downloads the selected files or folders to the local folder.
Bookmark	Creates a new bookmark to the current File Share location.
Bookmarks	Displays a list of files and folders that you have bookmarked.
Logout	Logs out of the File Share service.

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.

Topics:

- [Displaying the Network Explorer Page](#)
- [Working with Folders](#)
- [Working with Files](#)

Displaying the Network Explorer Page

You can display the 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](#)
- [Downloading a folder](#)
- [Copying Folders](#)
- [Cut and Paste a Folder](#)
- [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 Network Explorer page, do one of the following:
Click the name of the folder in which you want to create a new folder and click **New** from the top menu.
OR
Right-click the folder and select **New** option.
The below dialog is displayed.

The image shows a dialog box with a dark header bar containing the text 'NEW FOLDER NAME'. Below the header is a white area with a dashed orange rectangular border for text input. At the bottom of the dialog are two buttons: a light gray 'Cancel' button and an orange 'Create' button.

2. In the **New folder name** dialog, type the name of the folder you want to create.
3. Click **Create**.
A new folder is created.

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.
OR
Right-click the folder and select **Rename** option.
The name of the folder becomes editable.
3. Type a new name for the folder.
4. Click .

Downloading a folder

You can download the current folder to your local computer.

1. In the right pane of the Network Explorer page, click the name of the folder you want to download.
2. Click **Download** from the top menu.
OR
Right-click the folder and select **Download folder** option.
The folder is downloaded in a zip format.
In most web browsers, a dialog box appears prompting you to save or open the file.

Copying Folders

You can copy a folder and paste it into another folder.

1. In the right pane of the Network Explorer page, select the folder you wish to copy.
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:

- Click the **Copy** button from the top menu.
 - Right-click the file and select **Copy** option.
3. Open the folder in which you wish to paste. Do one of the following to paste the folder:
 - Click the **Paste** button from the top menu.
 - Right-click and select **Paste** option.

Cut and Paste a Folder

You can cut a folder and paste it into another folder.

1. In the right pane of the Network Explorer page, select the folder you wish to cut.
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:
 - Click the **Cut** button from the top menu.
 - Right-click the folder and select **Cut** option.
3. Open the folder in which you wish to paste. Do one of the following to paste the folder:
 - Click the **Paste** button from the top menu.
 - Right-click and select **Paste** option.

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** from the top menu.
OR
Right-click the folder and select **Delete** option.
3. Click the **Delete** button to confirm that you want the folder deleted.

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

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](#)
- [Copying Files](#)
- [Cut and Paste 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.

① **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, select the file you want to download.
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. Click **Download** from the top menu.
OR
Right-click on the file and select **Download** option.
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.

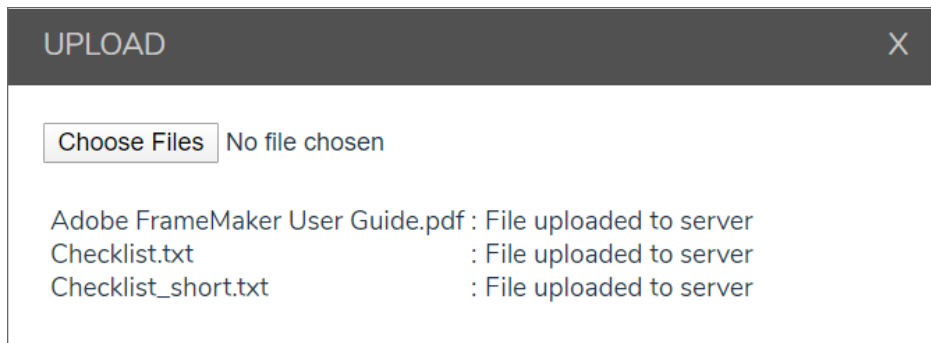
1. In the left navigation pane of the Network Explorer page, click the name of the folder to which you want to upload the files.
2. Click **Upload** from the top menu.
OR

Right-click the folder and select **Upload** option.

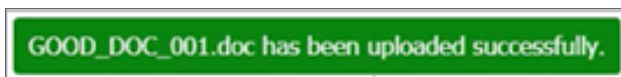
3. In the **Upload** box, click **Choose Files** to locate the files you want to upload from your computer.
4. Click **Open**.

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:



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



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



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

OR

To upload the files, drag and drop the files from your computer into the current folder.

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.
OR
Right-click the file and select **Rename** option.
The name of the file becomes editable.
3. Type a new name for the file.

4. Click .

Copying Files

You can copy files from one folder and paste it into another folder.

1. In the right pane of the Network Explorer page, select the files you wish to copy.
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:
 - Click the **Copy** button from the top menu.
 - Right-click the file and select **Copy** option.
3. Open the folder in which you wish to paste. Do one of the following to paste the files:
 - Click the **Paste** button from the top menu.
 - Right-click and select **Paste** option.

Cut and Paste Files

You can cut the files from a folder and paste it into another folder.

1. In the right pane of the Network Explorer page, select the files you wish to cut.
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:
 - Click the **Cut** button from the top menu.
 - Right-click the folder and select **Cut** option.
3. Open the folder in which you wish to paste. Do one of the following to paste the files:
 - Click the **Paste** button from the top menu.
 - Right-click and select **Paste** option.

Deleting Files

You can delete files from a folder.

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 **Delete** from the top menu.
OR
Right-click the file and select **Delete** option.
You are prompted to confirm the deletion.
3. Click **Delete**.

Network Explorer will completely delete the files from the remote machine. These items are not sent to the recycle bin on either machine and are not recoverable.

Secure Endpoint Manager (SEM)

SEM is the client application responsible for evaluating EPC, launching agents and bookmarks. SEM registers a custom URL scheme that gets invoked from browser for the specific tasks. SEM has two modules namely, Web Agent and Connect Agent.

Unified Web Agent for Workplace or browser access

From 12.4.3 onwards, the unified client has two modules namely, **Web Agent** and **Connect Agent**.

- Web Agent : This unified client is responsible for handling the following:
 - End point control: Performing the end point control checks.
 - Agent installation: Installation and updating connect tunnel.
 - Agent activation: Auto activate OnDemand Proxy and OnDemand Tunnel.
- Connect Agent: This unified client is responsible for handling bookmarks from WorkPlace. This client also provides backward compatibility if someone accesses WorkPlace on prior 12.4 versions.

① | **NOTE:** SEM is not displayed as tray icon in the system tool bar.

Topics:

- [Supported Operating Systems and Browsers](#)
- [Installing Secure Endpoint Manager](#)
- [Setting up the Secure Mobile Access Connect Agent](#)

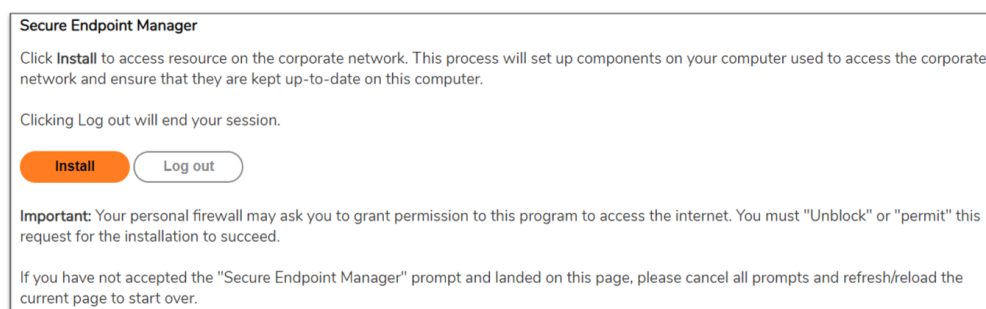
Supported Operating Systems and Browsers

The Secure Mobile Access Connect Agent supports these operating systems and browsers:

Operating System	Browser	Version
Windows 11	Edge	Version 113.0 or later
Windows 10	Chrome	Version 113.0 or later
	Firefox	Version 113.0 or later
macOS 14.X	Safari	Version 16.0 or later
macOS 13.X	Chrome	Version 113.0 or later
macOS 12.X		
macOS 11.X		

Installing Secure Endpoint Manager

On the Welcome page, the install and log out notification displays when you need to launch any native applications:

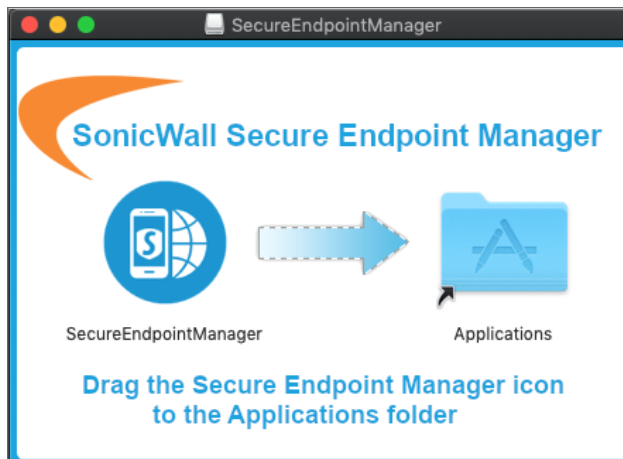


To install the SEM:

1. On the Welcome page, click **Install**.

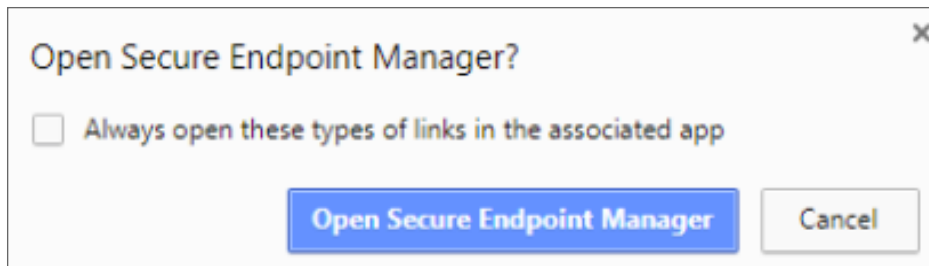
Based on your computer operating system, an installer is downloaded.

The Windows installer is `SecureEndPointManager.exe`, and the Macintosh installer is `SecureEndPointManager.dmg`. After the download is complete, the Windows installer needs your permission to install and the Macintosh installer guides you to copy the Secure Mobile Access Connect Agent in the `/Application` directory.

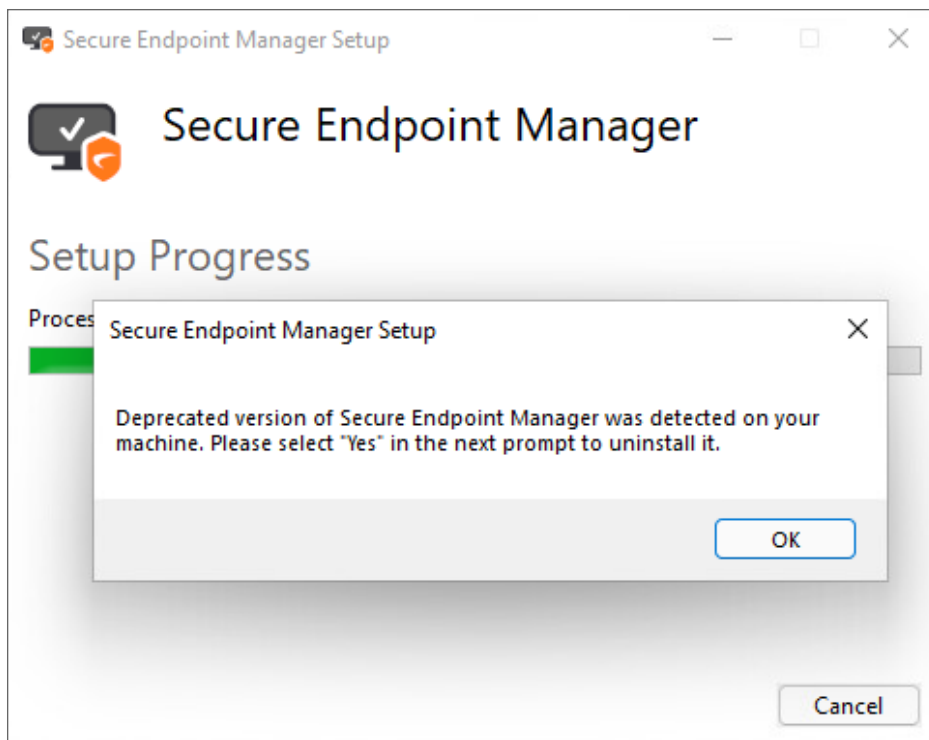


2. Once the download is complete, run the downloaded installer file.
3. In the confirmation dialog box, click **Run**.
4. On the Welcome page, click **Continue**.

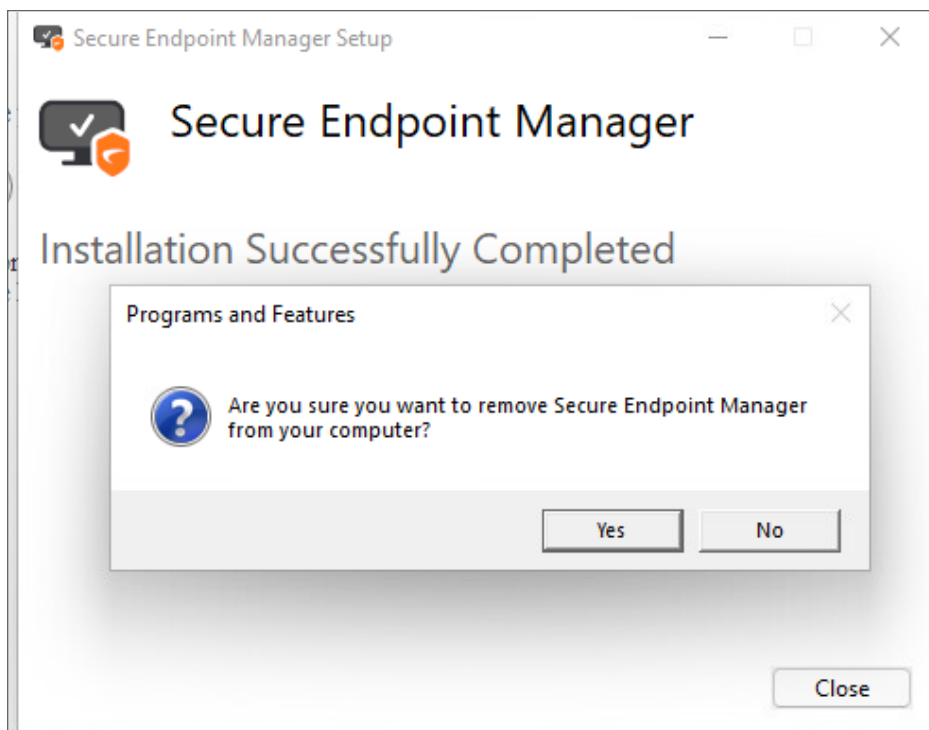
Based on your web browser, the application could pop up a warning message to confirm that you want to launch the Secure Mobile Access Connect Agent. For more information, see [Browser Warning](#).



5. Click **Open Secure Endpoint Manager** to launch the Secure Mobile Access Connect Agent.
 - ① **NOTE:** After successful installation of Secure Endpoint Manager, the unified client checks for deprecated version of agents in the client. If deprecated agents are present a message is displayed to remove the deprecated agents.



- Click **Yes** to remove the deprecated version of SEM.



Setting up the Secure Mobile Access Connect Agent

Topics:

- [Proxy Configuration](#)
- [Logs](#)
- [Browser Warning](#)
- [End Point Control \(EPC\)](#)
- [Personal Device Authorization\(PDA\)](#)

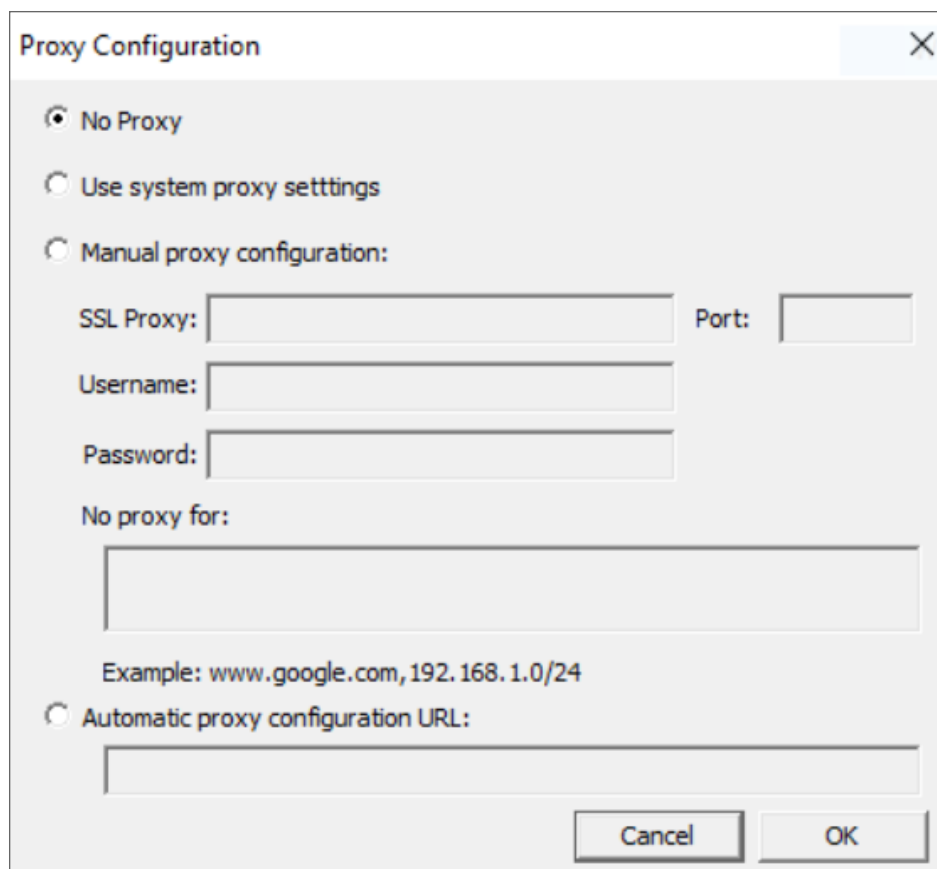
Proxy Configuration

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**

A screenshot of a 'Proxy Configuration' dialog box. It has a title bar with a close button (X). The dialog contains three radio button options: 'No Proxy' (selected), 'Use system proxy settings', and 'Manual proxy configuration:'. Below the 'Manual proxy configuration' option are input fields for 'SSL Proxy:', 'Port:', 'Username:', and 'Password:'. Below these is a section labeled 'No proxy for:' with a large text input field. An example text 'Example: www.google.com, 192.168.1.0/24' is shown below the input field. At the bottom, there is a radio button for 'Automatic proxy configuration URL:' followed by another large text input field. At the very bottom right are 'Cancel' and 'OK' buttons.

Proxy Configuration

☒ No Proxy

☐ Use system proxy settings

☐ Manual proxy configuration:

SSL Proxy: Port:

Username:

Password:

No proxy for:

Example: www.google.com, 192.168.1.0/24

☐ Automatic proxy configuration URL:

Cancel OK

Logs

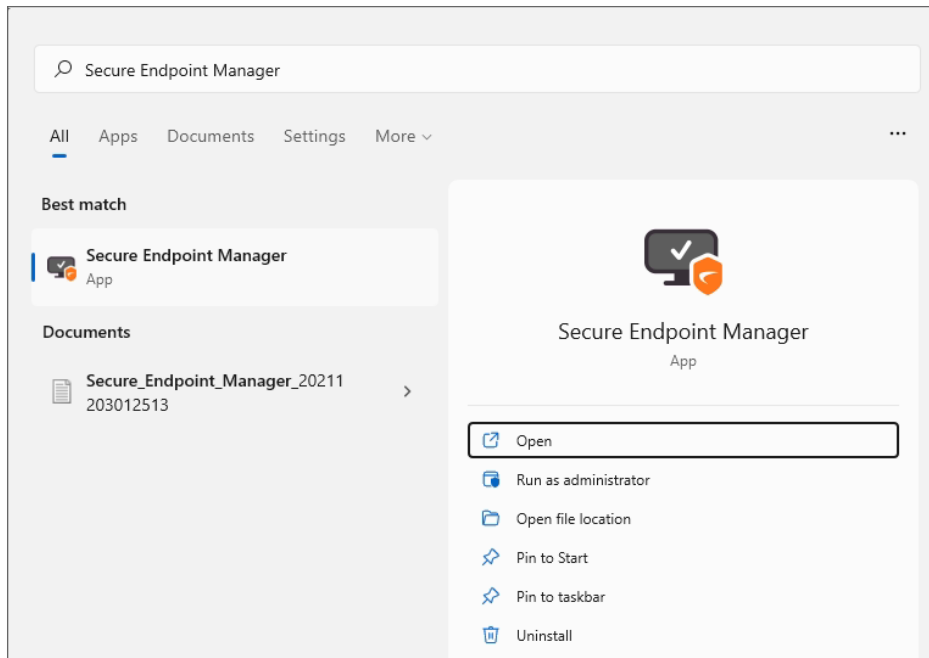
There is a Log tray on the system tool bar. You can right-click the tray and select the pop-up menu to view the logs.

Exporting logs in SEM

From 12.4.3 onwards, you can clear or export the system logs.

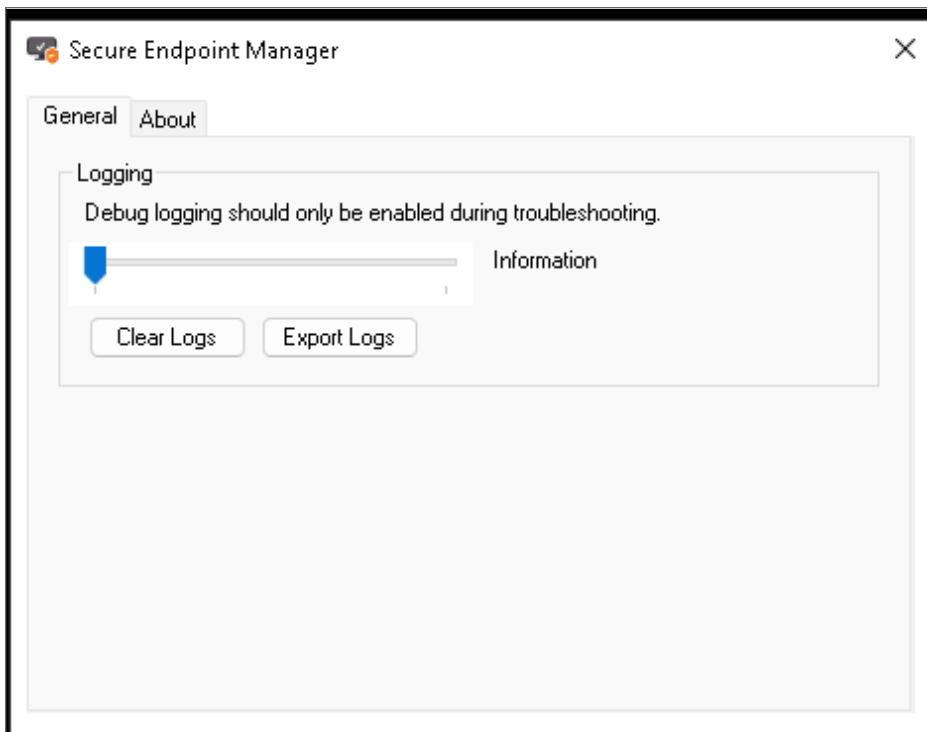
To clear or export logs in SEM:

1. In start menu, select **Secure Endpoint Manager** application.



① **TIP:** You can go to **AppData > Local > Programs > SonicWall > Secure Endpoint Manager** to find the **Secure Endpoint Manager** package.

2. Click **Open**.
3. In **General** Tab, set the log level to either to clear or export the debug logs or information.



4. Under **Logging** you can do the following:

- Click **Clear Logs** to clear the debug logs or information.
- Click **Export Logs** to export the debug logs or information.

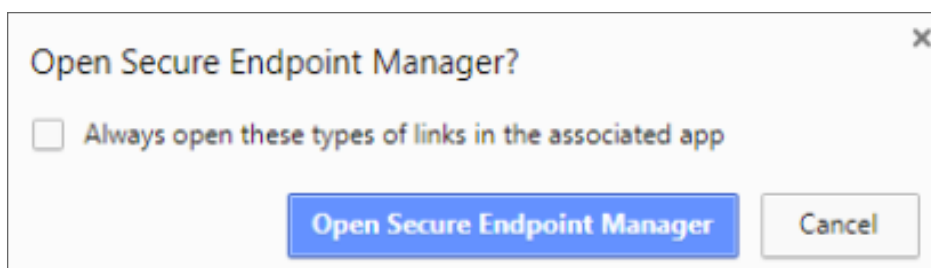
The logs or information files are downloaded.

① **TIP:** You can also go to **AppData > Local > SonicWall > SnwWebAgent** location to collect the logs.

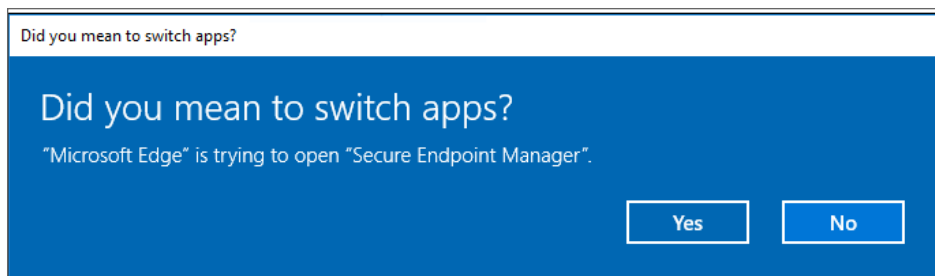
Browser Warning

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:

In a Chrome warning window, click **Open Secure Endpoint Manager** to launch the Secure Mobile Access Connect Agent.

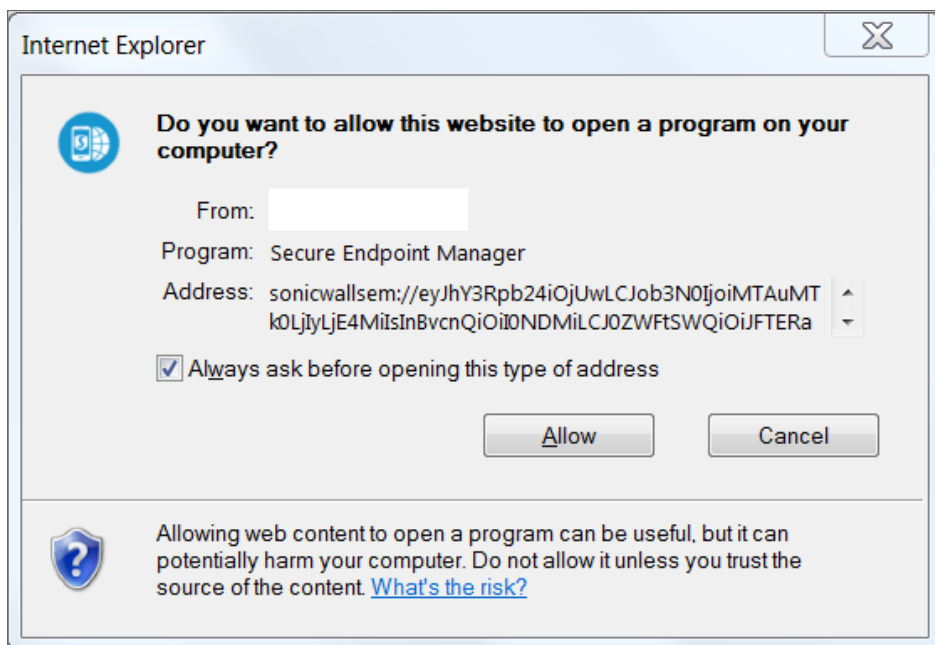


In Microsoft Edge warning window, click **Yes** to launch the Secure Mobile Access Connect Agent.

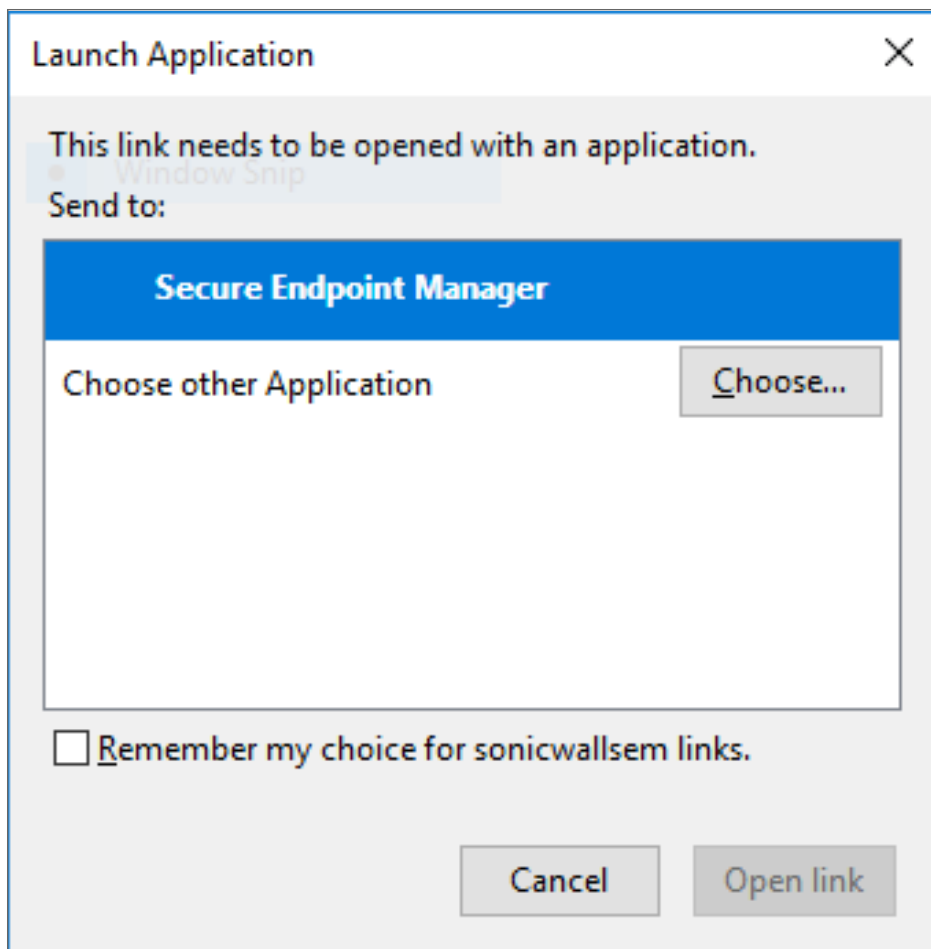


In an Internet Explorer warning window, click **Allow** to launch the Secure Mobile Access Connect Agent.

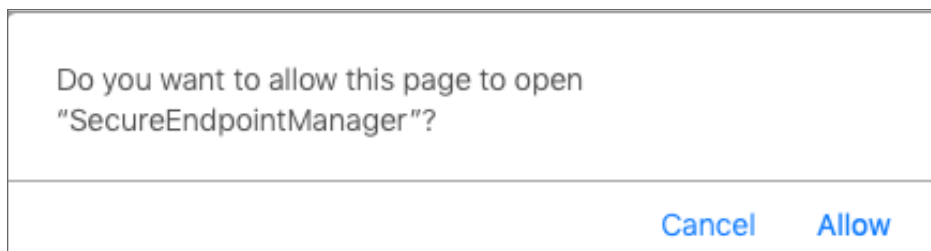
① **NOTE:** Since Microsoft is ending the support for Internet Explorer and for security reasons, using WorkPlace in Internet Explorer browser is not recommended.



In Firefox warning window, select **Endpoint Manager** and click **Open link** to launch the Secure Mobile Access Connect Agent.



In Safari warning window, click **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 your Administrator enables the EPC check option, 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.

Personal Device Authorization(PDA)

The Secure Mobile Access connect agent helps the PDA feature get the local machine's information. This option is available only if your administrator enables the PDA feature. Secure Mobile Access connect gets the information of the local machine and sends the information to the appliance.

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 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 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:

- 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, 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.

SonicWall Support

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

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 and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services at <https://sonicwall.com/pes>.
- 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

Secure Mobile Access for Workplace User Guide
Updated - January 2024
Software Version - 12.4
232-005701-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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. 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/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. 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
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035