SonicWall™
Secure Mobile Access 8.6

User Guide

SMA 200/400

SRA 1600/4600

SMA 500v Virtual Appliance

SONICWALL™

Copyright © 2017 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

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/.

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 User Guide
Updated - October 2017
Version - 8.6
232-003818-00 Rev B

Contents

Part 1. Introduction

About the Secure Mobile Access User Guide 7
Organization of this Guide 7
Guide Conventions 8

Virtual Office Overview 9
About Virtual Office 9
Accessing Virtual Office resources 9
Browser requirements 10
About certificates 12
About the Virtual Office Web Interface 13
Logging Out of the Virtual Office 16

Part 2. Using Secure Remote Access Features

Using Secure Mobile Access Connect Agents 18
What is the Secure Mobile Access Connect Agent? 18
Supported Operating Systems 18
Downloading and Installation 19
Setting up the SMA Connect Agent 20

Using Virtual Office Authentication 23
Importing Certificates 23
Using Two-Factor Authentication 23
User Prerequisites 24
RSA Two-Factor user authentication process 24
VASCO two-factor user authentication process 26
Using one-time passwords 27
User prerequisites 27
Logging in with a one-time password 27
Configuring one-time passwords for SMS-capable phones 28
Verifying user one-time password configuration 29

Using NetExtender 30
User Prerequisites 30
Using Mobile Connect 31
User configuration tasks 32
Installing NetExtender using the Mozilla Firefox browser 33
Installing NetExtender using the Internet Explorer browser 35
Installing NetExtender Using the Chrome Browser 37
Launching NetExtender Directly from Your Computer 40
Pre-filling the Server and Domain Fields while Installing NetExtender through Microsoft Installer 40
Configuring NetExtender Properties 42

Configuring NetExtender Connection Scripts 44
Configuring Batch File Commands 44
Configuring Proxy Settings 45
Configuring NetExtender Log Properties 47
Configuring NetExtender Advanced Properties 48
Configuring NetExtender Acceleration Properties 49
Configuring NetExtender Packet Capture Properties 49
Configuring Language Properties 50
Viewing the NetExtender Log 51
Disconnecting NetExtender 51
Upgrading NetExtender 52
Changing Passwords 52
Authentication Methods 52
Uninstalling NetExtender 53
Verifying NetExtender operation from the System Tray 53
Using the NetExtender Command Line Interface 54
Installing NetExtender on Linux 55
Using NetExtender on Linux 57

Using Secure Virtual Assist and Virtual Meeting 61
Using Secure Virtual Assist 61
Installing and Launching Secure Virtual Assist 62
Configuring Secure Virtual Assist Settings 63
Selecting a Secure Virtual Assist Mode 67
Launching a Secure Virtual Assist Technician Session 68
Performing Secure Virtual Assist Technician Tasks 70
Initiating a Secure Virtual Assist Session from the Customer View 77
Using Secure Virtual Assist 85
Using Secure Virtual Assist in Unattended Mode 87
Using Virtual Access Mode 88
Enabling a System for Secure Virtual Access 88
Using the Request Assistance Feature 92
Using Secure Virtual Meeting 92
Overview of Roles 93
Coordinator Role 94
Participant Role 114

Using File Shares 117
Using the File Shares Applet 117
User Prerequisites 117
Configuration Overview 118
Using HTML-based File Shares 119

Managing Bookmarks 123
Adding Bookmarks 123
RDP Bookmarks 126
Citrix Bookmarks 130
Web Bookmarks 132

Mobile Connect Bookmarks . . . 133
FTP Bookmarks . . . 133
SSHv2 Bookmarks . . . 133
Editing Bookmarks . . . 133
Removing Bookmarks . . . 134
Using Bookmarks . . . 134
Using Remote Desktop Bookmarks . . . 134
Using VNC Bookmarks . . . 137
Using Citrix Bookmarks . . . 138
Using Web Bookmarks . . . 139
Using Mobile Connect Bookmarks . . . 139
Using File Share Bookmarks . . . 140
Using FTP Bookmarks . . . 140
Using Telnet Bookmarks . . . 143
Using SSHv2 Bookmarks . . . 143
Global Bookmark Single Sign-On Options . . . 145
Per-Bookmark Single Sign-On Options . . . 145

Part 3. Appendix

Warranty and License Agreements . . . 149
GNU General Public License (GPL) Source Code . . . 149
Limited Hardware Warranty . . . 149
End User License Agreement . . . 150

SonicWall Support . . . 156

Part 1

Introduction

- About the Secure Mobile Access User Guide
- Virtual Office Overview

1

About the Secure Mobile Access User Guide

Welcome to the *SonicWall Secure Mobile Access (SMA) User* documentation. This document provides information on using the Secure Mobile Access user portal called Virtual Office that allows you to create bookmarks and run services over the SMA/SRA appliance.

Check the SonicWall documentation Web site for the latest versions of all SonicWall product documentation at https://support.sonicwall.com/sonicwall-secure-mobile-access/sma%206200/release-notes-guides.

Organization of this Guide

The SonicWall Secure Mobile Access User Guide is structured into the following parts:

Chapter 1 About the Secure Mobile Access User Guide

This chapter provides helpful information for using this guide. It includes conventions used in this guide, information on how to obtain additional product information, and a Quick Access Worksheet that you should complete before using the SMA/SRA appliance.

Chapter 2 Virtual Office Overview

This chapter provides an overview of SMA/SRA appliance user features, NetExtender, File Shares, Secure Virtual Assist, Secure Virtual Access, Secure Virtual Meeting, services, sessions, bookmarks, and service tray menu options.

Chapter 3 Using Secure Mobile Access Connect Agents

This chapter provides procedures on importing certificates, using Two-Factor authentication, and using One-Time Passwords.

Chapter 4 Using Virtual Office Authentication

This chapter provides details on how to use the authentication features of theSonicWall Secure Mobile Access (SMA) Virtual Office portal.

Chapter 5 Using NetExtender

This chapter provides procedures on installing, configuring, and using NetExtender.

Chapter 6 Using Secure Virtual Assist and Virtual Meeting

This chapter provides procedures on installing and using Secure Virtual Assist and Secure Virtual Meeting.

Chapter 7 Using File Shares

This chapter provides procedures on using file shares.

Chapter 8 Managing Bookmarks

This chapter provides procedures on configuring bookmarks.

Appendix A Warranty and License Agreements

This appendix provides the Limited Hardware Warranty and End User Licensing Agreement, and SonicWall Support contact information.

Guide Conventions

The conventions used in this guide are as follows:

Guide Conventions

Convention	Use
Bold	Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.

2

Virtual Office Overview

This section provides an overview of the SonicWall Secure Mobile Access (SMA) user portal, the Virtual Office. It also includes information about supported browsers and associated requirements.

Topics:

- About Virtual Office on page 9
- Browser requirements on page 10
- About certificates on page 12
- About the Virtual Office Web Interface on page 13
- Logging Out of the Virtual Office on page 16

About Virtual Office

Secure Mobile Access Virtual Office provides secure remote access to network resources, such as applications, files, intranet web sites, and email through web access interfaces such as Microsoft Outlook Web Access (OWA). The underlying protocol used for these sessions is SSL.

With Secure Mobile Access, mobile workers, telecommuters, partners, and customers can access information and applications on your intranet or extranet. What information should be accessible to the user is determined by access policies configured by the Secure Mobile Access administrator.

Accessing Virtual Office resources

Remote network resources can be accessed in the following ways:

- **Using a standard Web browser** - To access network resources, you must log in to the Secure Mobile Access portal. After authenticated, you might access intranet HTTP and HTTPS sites, offloaded portals, Web-based applications, and Web-based email. In addition, you might upload and download files using FTP or Windows Network File Sharing. All access is done through a standard Web browser and does not require any client applications to be downloaded to remote users' machines.
- **Using Java thin-client access to corporate desktops and applications** – The SonicWall SMA/SRA security appliance includes several Java or ActiveX thin-client programs that can be launched from within the SonicWall SMA/SRA security appliance. Terminal Services and VNC Java clients allow remote users to access corporate servers and desktops, open files, edit and store data as if they were at the office. Terminal Services provides the ability to open individual applications and support remote sound and print services. In addition, users might access Telnet and SSH servers for SSH version 1 (SSHv1) and SSH version 2 (SSHv2), from the Secure Mobile Access portal.
- **Using the NetExtender Secure Mobile Access client** – The SonicWall Secure Mobile Access network extension client, NetExtender, is available through the Secure Mobile Access Virtual Office portal through an ActiveX control or through standalone applications for Windows, Linux, and Mac OS X platforms. To connect using the SMA/SRA client, log in to the portal, download the installer application

and then launch the NetExtender connector to establish the SSL VPN tunnel. About the Virtual Office Web Interface on page 13. After you have set up the SSL VPN tunnel, you can access network resources as if you were on the local network.

The NetExtender standalone applications are automatically installed on a client system the first time you click the NetExtender link in the Virtual Office portal. The standalone client can be launched directly from users' computers without requiring them to log in to the Secure Mobile Access portal first.

- **Using the SonicWall Mobile Connect app** – SonicWall Mobile Connect is an app for iOS, Android, Mac OS X, Windows Phone, Windows 10, and ChromeOS that, like NetExtender, uses SSL VPN to enable secure, mobile connections to private networks protected by SonicWall security appliances. For information about installing and using SonicWall Mobile Connect, see the *SonicWall Mobile Connect User* documentation available at:
  https://support.sonicwall.com/sonicwall-secure-mobile-access/sma%206200/release-notes-guides

For secure remote access to work as described in this guide, the SonicWall SMA/SRA security appliance must be installed and configured according to the directions provided in the *Getting Started Guide* for your model.

NOTE: If your Administrator has Remediation enabled, the warning message "Access is denied by Geo IP & Botnet Filter" displays when attempting to accessing remote network resources. A browser window is automatically opened to display a CAPTCHA picture and entry field. You must complete remediation within the specified time limit before you can login. Refer to the *SonicWall Secure Mobile Access Administration* documentation for details.

Browser requirements

the Browser Versions Per Client Operating Systems table provides information about the browsers supported on various client operating systems.

Browser Versions Per Client Operating Systems

Browser	Operating System	
Internet Explorer 11	Windows 7	
Internet Explorer 10	Windows 10	
Internet Explorer 11	Windows 10	
Mozilla Firefox (latest version)	Windows Vista	Windows 10
	Windows 7	Linux
	Windows 10	Mac OS X
Google Chrome (latest version)	Windows Vista	Windows 10
	Windows 7	Linux
	Windows 10	Mac OS X
Apple Safari (latest version)	Mac OS X	

For Administrator management interface browser compatibility, refer to the *SonicWall Secure Mobile Access Administration* documentation.

Below, the Browser Support For Virtual Office Features table provides browser requirements for specific features of Virtual Office.

Browser Support For Virtual Office Features

Application Proxy Features & Browser Requirements	Windows 7	Windows 10	Linux	Mac OS X
NetExtender			Browser Independent	
RDP5				
VNC				
Telnet				
SSHv2				
HTTP, HTTPS, FTP (Browser)				
File Sharing (Browser)				
File Sharing				

Browser Support For Virtual Office Features (Continued)

Application Proxy Features & Browser Requirements	Windows 7	Windows 10	Linux	Mac OS X
Citrix				
Virtual Assist			Browser Independent	Browser Independent
HTML5 (Internet Explorer 11 and later)				

Virtual Assist is fully supported on Windows platforms. Virtual Assist is certified to work on Windows 7, and Windows Vista. Limited functionality is supported on Mac OS where customers can request for assistance through web-requests.

NOTE: If you are using an HTML5 client with Internet Explorer, it must be IE11 or later. Earlier versions of Internet Explorer do not support HTML5.

NOTE: Not all HTML5 features (such as Audio Redirect) are supported on Internet Explorer because of browser limitations.

NOTE: Plug-ins might not be supported in Firefox or Chrome browsers, because of the removal of NPAPI support. To launch clients such as NetExtender and Virtual Assist, download and open the files manually.

About certificates

If the SMA/SRA appliance uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWall recommends that you import the certificate. The easiest way to import the certificate is to click **Import Certificate** on the **System > Certificates** page.

If the certificate is not issued by an authorized organization, a message is displayed warning users of the risk. A user can then view detailed information and choose to continue or end the connection.

When using the network logon method from the Windows login screen, NetExtender uses System Store for certificate-based authentication. When the user is already logged in to Windows, NetExtender uses the User Store for certificate-based authentication. A user who wants to use the network logon method when certificate authentication is also enabled should import his user certificate into the System Store as well as into the User Store.

About the Virtual Office Web Interface

You can access the Virtual Office portal at the URL provided to you by your network administrator.

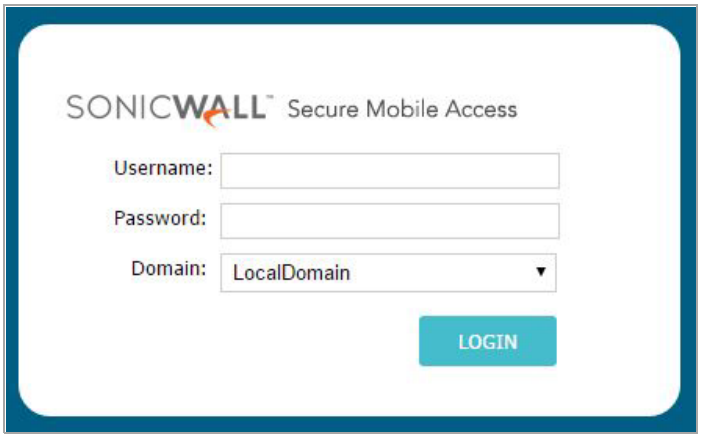
To log in to Virtual Office:

1 On your workstation at your remote location, launch an approved browser and enter the IP address of the Virtual Office portal in the **Location** or **Address** field. By default, this is the default LAN IP address of the SMA/SRA appliance, **https://192.168.200.1**.

2 A security warning should appear. Click **Yes** to continue.

3 The SonicWall Secure Mobile Access login page displays and prompts you to enter your user name and password. To log in using the default administrator credentials, enter **admin** in the **User Name** field, **password** in the **Password** field, and select a domain from the **Domain** drop-down list and click **Login**. Only **LocalDomain** allows Administrator privileges.

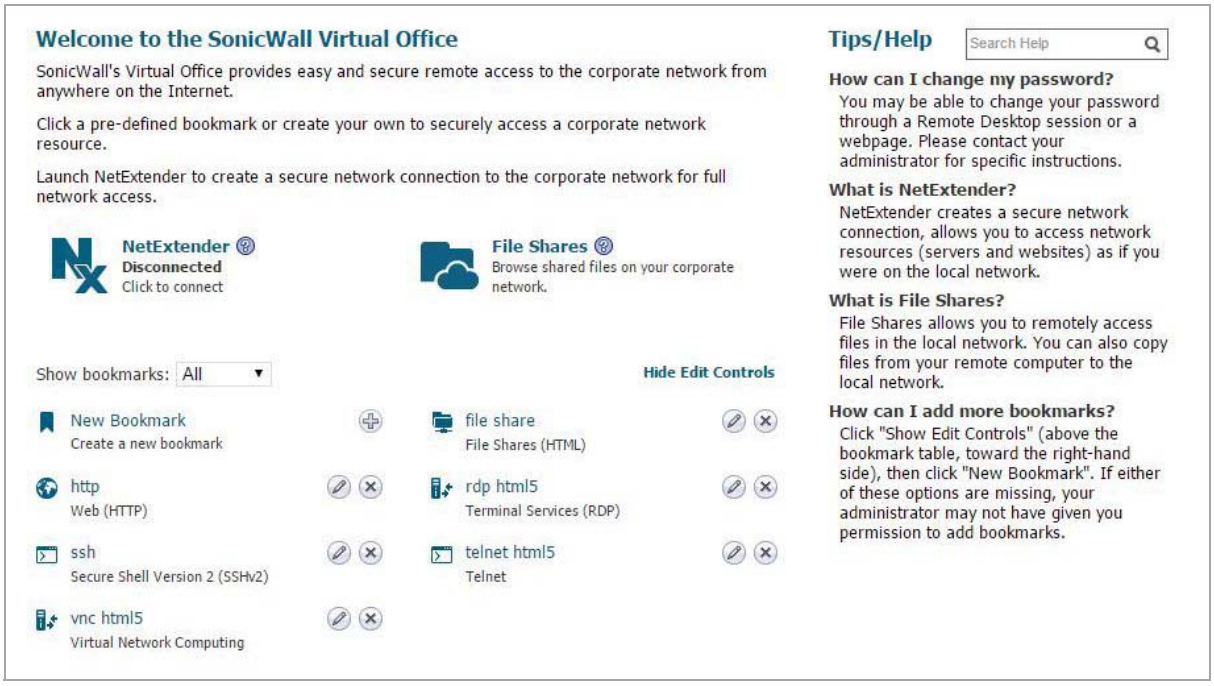
NOTE: Your Administrator might have set up another login and password for you that has only user privileges.



The default page displayed is the Virtual Office home page. The default version of this page shows a SonicWall logo, although your company's system Administrator might have customized this page to contain a logo and look and feel of your company. Go to the About Virtual Office on page 9 to learn more about the Virtual Office home page.

From the Virtual Office portal home page, you cannot navigate to the Administrator's environment. If you have Administrator's privileges and want to enter the Administrator environment, you need to go back to the login page and enter a username and password that have Administrator privileges, and log in again using the LocalDomain domain. Only the LocalDomain allows Administrator access to the management interface. Also note that the domain is independent of the privileges set up for the user.

Logging in as a user takes you directly to Virtual Office. The Virtual Office Home page displays as shown here.



The Virtual Office content varies based on the configuration of your network administrator. Some bookmarks and services described in the *SonicWall Secure Mobile Access User* documentation might not be displayed when you log in to the SMA/SRA security appliance.

The Virtual Office can contain any of the nodes described in the Virtual Office Node Descriptions table.

Virtual Office Node Descriptions

Node	Description
File Shares	Provides access to the File Shares utility that gives remote users with a secure Web interface access to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.
NetExtender	Provides access to the NetExtender utility, a transparent SSL VPN client for Windows or Linux users that allows you to run any application securely on the remote network. It acts as an IP-level mechanism provided by the virtual interface that negotiates the ActiveX component (on Windows with IE), using a Point-to-Point Protocol (PPP) adapter instance. On non-Windows platforms, Java controls are used to automatically install NetExtender from the Virtual Office portal. After installation, NetExtender automatically launches and connects a virtual adapter for SSL secure NetExtender point-to-point access to permitted hosts and subnets on the internal network.
Secure Virtual Assist	Provides access to Virtual Assist, an easy to use tool that allows SonicWall Secure Mobile Access users to remotely support customers by taking control of their computers while the customer observes. Virtual Assist is a lightweight, thin client that installs automatically using Java from the Secure Mobile Access Virtual Office without requiring the installation of any external software. For computers that do not support Java, Virtual Assist can be manually installed by downloading an executable file from the Virtual Office.

Virtual Office Node Descriptions (Continued)

Node	Description
Secure Virtual Meeting	Provides access to Virtual Meeting that allows multiple users to view a desktop and interactively participate in a meeting from virtually anywhere with an Internet connection. Virtual Meeting is similar to the one-to-one desktop sharing provided by Virtual Assist except multiple users can share a desktop.
Secure Virtual Access (if configured by Administrator	Virtual Access allows Technicians to gain access to systems outside the LAN of the SMA/SRA appliance. After downloading and installing the thin client for Virtual Access mode, the system appears only on that Technician's Virtual Assist support queue, within the Secure Mobile Access management interface.
All Bookmarks	Provides a list of available bookmarks which are objects that enable you to connect to a location or application conveniently and quickly.
Downloads	Provides a list of downloadable clients and applications.
Options	Provides the option to change user password and use single sign-on, if enabled by the Administrator.
Help	Launches online help for Virtual Office.
Tips/Help	Provides a short list of common questions and tips about the Virtual Office.
Logout	Logs you out of the Virtual Office environment.

The Home page provides customized content and links to network resources. The Home Page might contain support contact information, VPN instructions, company news, or technical updates.

Only a Web browser is required to access intranet web sites, File Shares, and FTP sites. VNC, and Telnet require Java. SSHv2 provide strong encryption, requires Oracle JRE 1.4 or above and can only connect to servers that support SSHv2. Terminal Services requires Java on the client machine.

As examples of tasks you can do and environments you can reach through Virtual Office, you can connect to:

- Intranet Web or HTTPS sites – If your organization supports Web-based email, such as Outlook Web Access, you can also access Web-based email
- The entire network by launching the NetExtender client
- FTP servers for uploading and downloading files
- The corporate network neighborhood for file sharing
- Telnet and SSH servers
- Desktops and desktop applications using Terminal Services or VNC.
- Email servers through the NetExtender client.

The Administrator determines what resources are available to users from the SonicWall Secure Mobile Access Virtual Office. The Administrator can create user, group, and global policies that disable access to certain machines or applications on the corporate network.

The Administrator might also define bookmarks, or preconfigured links, to Web sites or computers on the intranet. Additional bookmarks might be defined by the end user.

SonicWall NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

Logging Out of the Virtual Office

To end your session, simply return to the Virtual Office home page from wherever you are within the portal and click **Logout**.

When using the Virtual Office with the **admin** username, the **Logout** button is not displayed. This is a security measure to ensure that Administrators log out of the administrative interface, and not the Virtual Office.

Part 2

Using Secure Remote Access Features

- Using Secure Mobile Access Connect Agents
- Using Virtual Office Authentication
- Using NetExtender
- Using Secure Virtual Assist and Virtual Meeting
- Using File Shares
- Managing Bookmarks

3

Using Secure Mobile Access Connect Agents

This section provides details on how to use the features of the SonicWall Secure Mobile Access (SMA) Connect Agents portal.

Topics:

- What is the Secure Mobile Access Connect Agent? on page 18

What is the Secure Mobile Access Connect Agent?

The Browser Plug-ins (NPAPI, ActiveX, and Java Applet) are used to launch native applications such as Net-Extender, Virtual Assist, EPC and so on. For security reasons, popular browsers block theses 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 SMA Connect Agent uses the Scheme URL to replace the Browser Plug-ins. The SMA 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 SMA Connect Agent.

Topics:

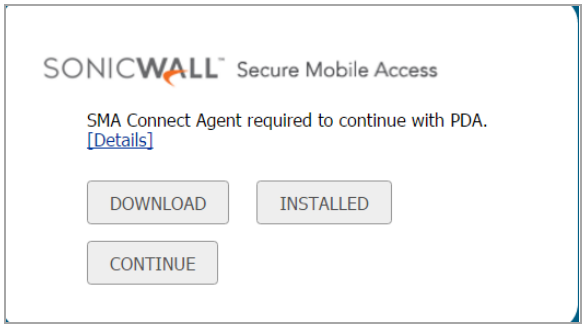
- Supported Operating Systems on page 18
- Downloading and Installation on page 19
- Setting up the SMA Connect Agent on page 20

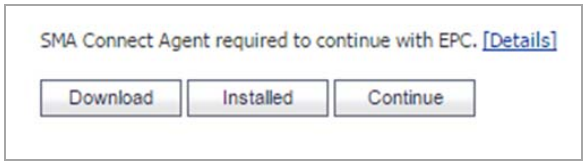
Supported Operating Systems

The SMA Connect Agent supports Windows (7, 8, and 10) as well as the Macintosh (OS X) operating systems.

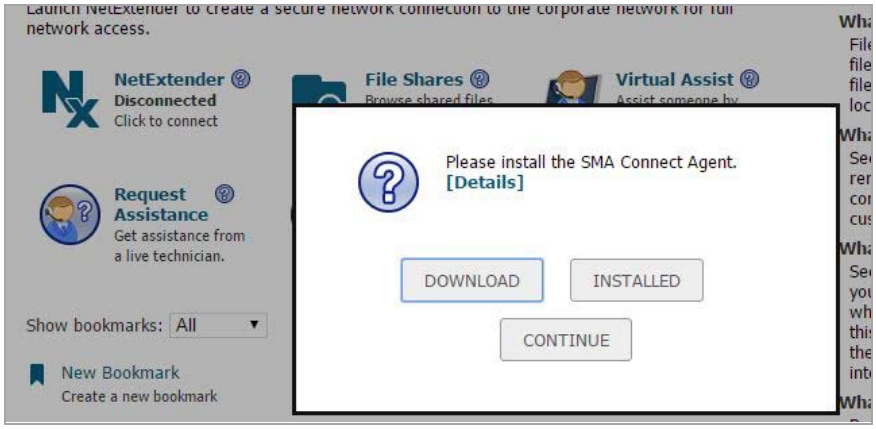
Downloading and Installation

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





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



- **Download** - Click Download to download and install SMA Connect Agent. After that, users can click Installed to tell the browser to 'remember' that the SMA 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 SMA 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 SMA Connect Agent in the `/Application` directory.

Setting up the SMA Connect Agent

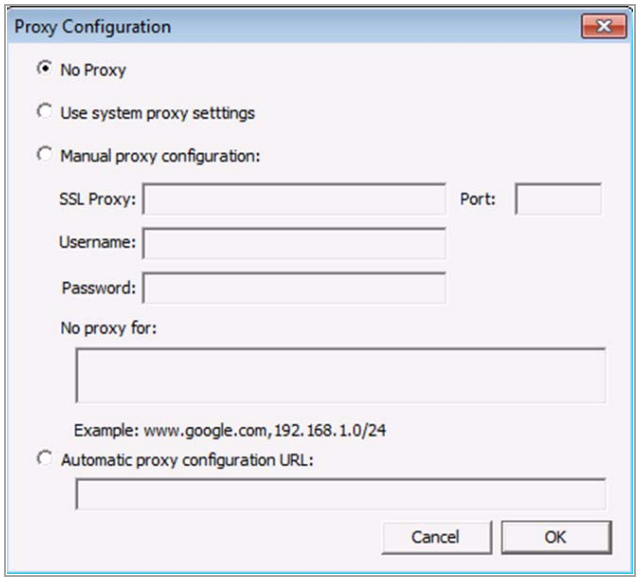
Proxy Configuration

SMA 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 SMA 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 SMA 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** -

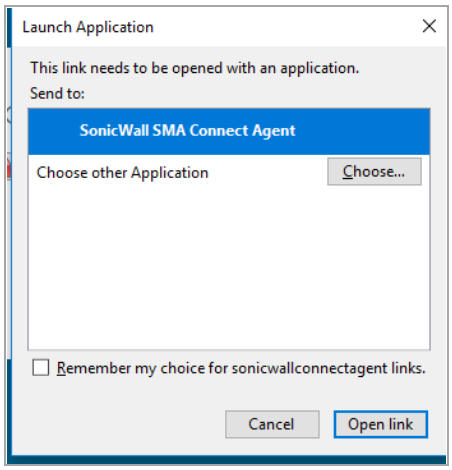


Logs

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.

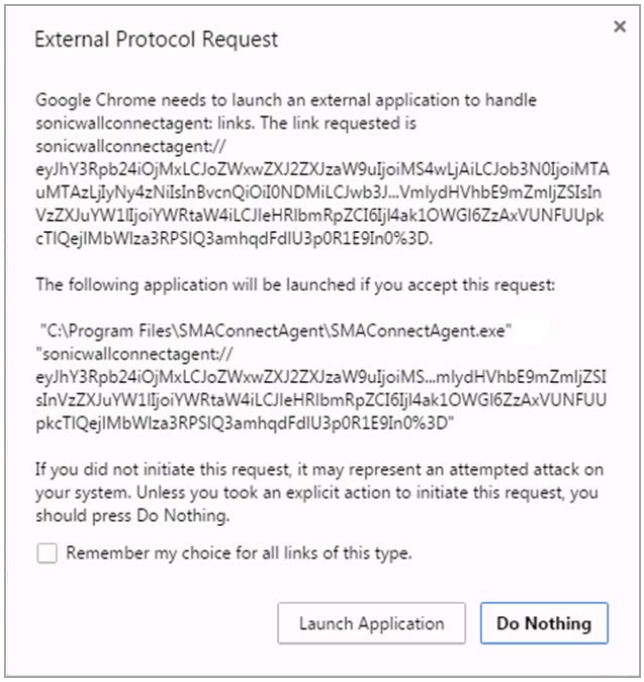
Browser Warning

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

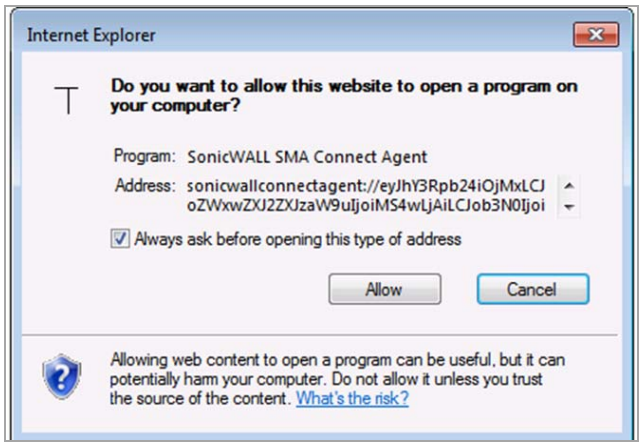


With a Firefox warning window, press **OK** to launch the SMA Connect Agent.

To launch 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.



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



In an Internet Explorer warning window, press Allow to launch the SMA Connect Agent.

End Point Control (EPC)

The SMA 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 SMA Connect Agent do the EPC check.

The SMA 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 SMA Connect Agent downloads/Installs or upgrades the EPC Service. After installing or upgrading, the SMA Connect Agent does the EPC check.

If the EPC feature (Appliance side) enables the “Show EPC failed message in detail at client side,” the SMA 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 SMA 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 SMA Connect Agent. SMA Connect gets the information of the local machine and sends the information to the appliance.

SonicWall Application

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

4

Using Virtual Office Authentication

This section provides details on how to use the authentication features of the SonicWall Secure Mobile Access (SMA) Virtual Office portal.

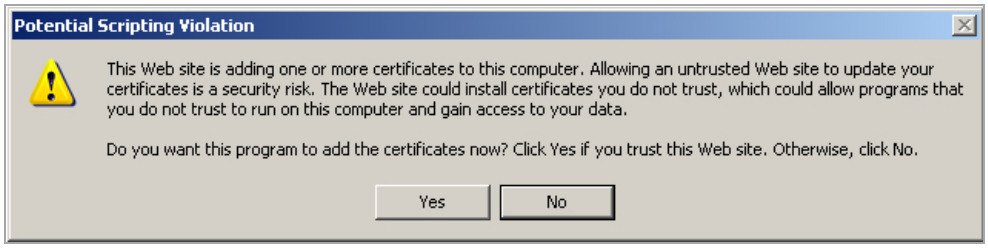
Topics:

- Importing Certificates on page 23
- Using Two-Factor Authentication on page 23
- Using one-time passwords on page 27

Importing Certificates

If the SMA/SRA appliance uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWall recommends that you import the certificate.

If using Internet Explorer, the easiest way to import the certificate is to click **Import Certificat**e at the bottom of the Virtual Office home page. The following warning messages can be displayed:



Click **Yes**. The certificate is imported.

NOTE: Certificates can only be imported through this method if you are using Internet Explorer. Certificates for other browsers such as Chrome or Firefox must be imported manually.

When using the network logon method from the Windows login screen, NetExtender uses System Store for certificate-based authentication. When the user is already logged in to Windows, NetExtender uses the User Store for certificate-based authentication. A user who wants to use the network logon method when certificate authentication is also enabled should import his user certificate into the System Store as well as into the User Store.

Using Two-Factor Authentication

The following sections describe how to log in to the Secure Mobile Access Virtual Office portal using two-factor authentication:

- User Prerequisites on page 24
- RSA Two-Factor user authentication process on page 24
- VASCO two-factor user authentication process on page 26

User Prerequisites

Before you can log in using two-factor authentication, you must meet the following prerequisites:

- Your Administrator has created your user account.
- You have an account with a two-factor authentication server that conforms to the RFC standard.

RSA Two-Factor user authentication process

The following sections describe user tasks when using RSA two-factor authentication to log in to the Secure Mobile Access Virtual Office:

- Logging into Virtual Office Using RSA Two-Factor Authentication on page 24
- Creating a new PIN on page 25
- Waiting for the next token on page 25

Logging into Virtual Office Using RSA Two-Factor Authentication

To log in to the SonicWall Secure Mobile Access Virtual Office using RSA two-factor authentication:

1 Enter the IP address of the SMA/SRA appliance in your browser. The authentication window is displayed.

2 Type your username into the **Username** field.

3 The first time you log in to the Virtual Office, your entry in the password field depends on whether your system requires a PIN:

- If you already have a PIN, enter the *passcode* in the **Password** field. The passcode is the user PIN and the SecurID token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
- If a PIN is required, but you do not yet have a PIN, enter the SecurID token code in the **Password** field. You are prompted to create a PIN.

- If the RSA server does not require a PIN, simply enter the SecurID token code.

NOTE: Consult with your network administrator to determine if your configuration requires a PIN.

4 Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.

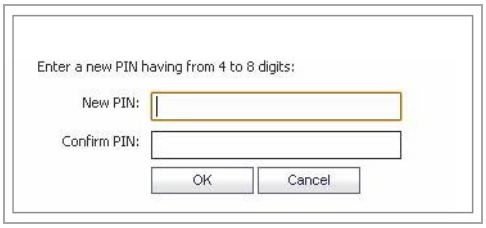
5 Click **Login**.

Creating a new PIN

The RSA Authentication Manager automatically determines when users are required to create a new PIN. The SMA/SRA appliance prompts the user to enter new PIN.

To create a new PIN:

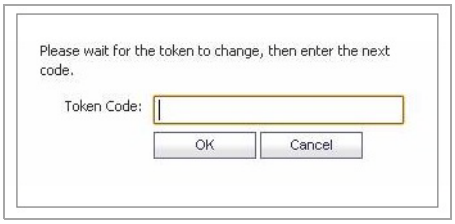
1 Enter the PIN in the **New PIN** field and again in the **Confirm PIN** field and then click **OK**. The PIN must be between four and eight characters long.



2 The RSA Authentication Manager verifies that the new PIN is acceptable. If the PIN is accepted, you are prompted to log in with the new passcode.

Waiting for the next token

If user authentication fails three consecutive times, the RSA server requires the user to enter a new token. To complete authentication, the user is prompted to wait for the token to change and enter the new token.



VASCO two-factor user authentication process

The following sections describe user tasks when using RSA two-factor authentication:

- Logging into Virtual Office using VASCO two-factor authentication on page 26
- Other RADIUS server two-factor authentication process on page 26

Logging into Virtual Office using VASCO two-factor authentication

To log in to the Secure Mobile Access Virtual Office using VASCO two-factor authentication:

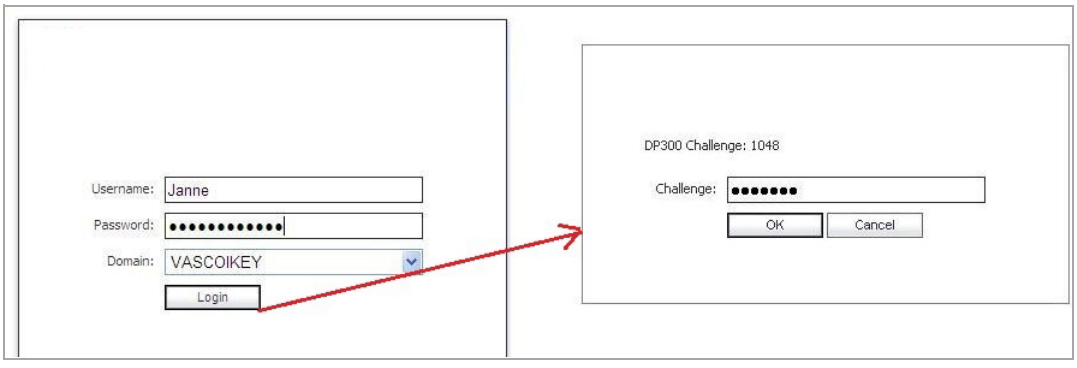
1. Enter the IP address of the SMA/SRA appliance in your browser. The authentication window is displayed.
2. Enter your username in the **Username** field.
3. Enter the passcode in the **Password** field. Your entry in the password field depends on whether your system requires a PIN:
   - If you already have a PIN, enter the *passcode* in the **Password** field. The passcode is the user PIN and the VASCO Digipass token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
   - If a PIN is required, but you do not yet have a PIN, enter the VASCO Digipass code in the **Password** field. You are prompted to create a PIN.
   - If the VASCO server does not require a PIN, simply enter the VASCO Digipass code.

   NOTE: Consult with your network Administrator to determine if your configuration requires a PIN.
4. Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.
5. Click **Login**.

Other RADIUS server two-factor authentication process

To log in to the Virtual Office using another type of RADIUS server for two-factor authentication:

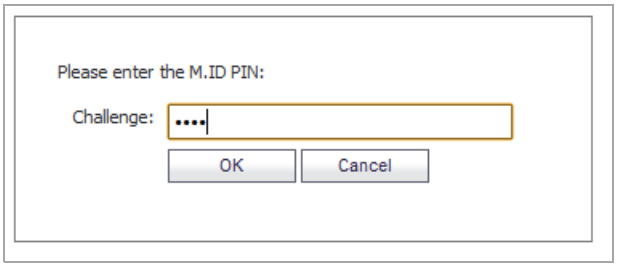
1. Enter the IP address of the SMA/SRA appliance in your browser. The authentication window is displayed.



2. Enter your username in the **Username** field.
3. Enter your password in the **Password** field.
4. Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.

5 Click **Login**.

6 You are prompted to enter additional information, the details of which depends on the type of RADIUS server used. The example below shows an M.ID RADIUS server that first prompts you to “Please enter the M.ID PIN.” Enter the PIN in the **Challenge** field and then click **OK**.



7 You are then prompted to “Please enter the M.ID Passcode.” Enter the passcode received through email or text message in the **Challenge** field and then click **OK**.

Using one-time passwords

The following sections describe how to use one-time passwords:

- User prerequisites on page 27
- Logging in with a one-time password on page 27
- Configuring one-time passwords for SMS-capable phones on page 28
- Verifying user one-time password configuration on page 29

User prerequisites

Users must have a user account enabled in the Secure Mobile Access management interface. Only users enabled by the Administrator to use the One-Time Password feature needs to use the following procedure to log in. The Administrator must enable a correct email address that is accessible by the user. Users cannot enable the One-Time Password feature themselves, and they must be able to access the Secure Mobile Access Virtual Office portal.

Logging in with a one-time password

To use the One-Time Password feature:

1 If you are not logged into the Secure Mobile Access Virtual Office user interface, open a web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**.

2 Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** drop-down menu.

3 Click **Login**.

4 The prompt “A temporary password has been sent to user@email.com” appears, displaying your pre-configured email account.

5 Log in to your email account to retrieve the one-time password.

6 Type or paste the one-time password into the **Password** field where prompted and then click **Login**.

You are logged in to the Virtual Office.

NOTE: One-time passwords are immediately deleted after a successful login, and cannot be used again. Unused one-time passwords expire according to each user’s time-out policy.

Configuring one-time passwords for SMS-capable phones

One-Time Passwords can be configured to be sent through email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS.

Below is a list of SMS email formats for selected major carriers, where 4085551212 represents a 10-digit telephone number and area code.

NOTE: These SMS email formats are for reference only. These email formats are subject to change and can vary. You might need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T: 4085551212@mobile.att.net
- Cingular: 4085551212@mobile.mycingular.com
- T-Mobile: 4085551212@tmomail.net
- Nextel: 4085551212@messaging.nextel.com
- Virgin Mobile: 4085551212@vmobl.com
- Qwest: 4085551212@qwestmp.com

For a more complete list, see the *SonicWall Secure Mobile Access Administration* documentation.

Verifying user one-time password configuration

If you are successfully logged in to Virtual Office, you have correctly used the One-Time Password feature.

If you cannot log in using the One-Time Password feature, verify the following:

- Are you able to log in to the Virtual Office without being prompted to check your email for a one-time password? If so, you have not been enabled to use the One-Time Password feature. Contact your Secure Mobile Access Administrator if you believe this is an error.
- Is your email address correct? If your email address has been entered incorrectly, contact your Secure Mobile Access Administrator to correct it.
- Is there no email with a one-time password? Wait a few minutes and refresh your email inbox. Check your spam filter. If there is no email after several minutes, try to log in again to generate a new one-time password.
- Have you accurately typed the one-time password in the correct field? Re-type or copy and paste the one-time password.

5

Using NetExtender

This section explains how to configure and use SonicWall NetExtender. Information about using Mobile Connect is also provided.

Topics:

- User Prerequisites on page 30
- Using Mobile Connect on page 31
- User configuration tasks on page 32

User Prerequisites

Prerequisites for Windows Clients:

Windows clients must meet the following prerequisites in order to use NetExtender:

- **One of the following platforms:**
  - **Windows 10, Windows 7, Windows 2012, Windows Server 2008 R2**
- **One of the following browsers:**
  - **Internet Explorer 9.0 and higher**
  - **Mozilla Firefox 16.0 and higher**
  - **Google Chrome 22.0 and higher**
- To initially install the NetExtender client, the user must be logged into the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the SMA/SRA gateway uses a self-signed SSL certificate for HTTPS authentication, it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure if the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWall recommends that you import the certificate. The easiest way to import the certificate is to click **Import Certificate** on the Virtual Office home page.

  When using the network logon method from the Windows login screen, NetExtender uses System Store for certificate-based authentication. When the user is already logged in to Windows, NetExtender uses the User Store for certificate-based authentication. A user who wants to use the network logon method when certificate authentication is also enabled should import his user certificate into the System Store as well as into the User Store.

Prerequisites for Mac OS X clients:

Mac OS X clients meet the following prerequisites in order to use NetExtender:

- Mac OS X 10.7 through 10.10

  NOTE: Mac NetExtender is End Of Support on El Capitan (10.11) and later. In future releases of SMA//SRA firmware, an error appears when a user tries to launch NetExtender, asking the user to install Mobile Connect from the App Store. Secure Mobile Access 8.1 is the final version that has Mac NetExtender support. SonicWall strongly recommends using SonicWall Mobile Connect for Mac OS X devices instead of NetExtender, currently and in future releases.

- **Java 1.7 and higher**
- Both PowerPC and Intel Macs are supported

Prerequisites for Linux clients:

Linux 32-bit or 64-bit clients are supported for NetExtender when running one of the following distributions (32-bit or 64-bit):

- **Linux Fedora Core 20 or higher, Ubuntu 12.04, 13.10, or higher, or OpenSUSE 10.3 or higher**
- **Java 1.7 and higher is required for using the NetExtender user interface**

The NetExtender client has been known to work on other distributions as well, but these are not officially supported.

NOTE: Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5 or higher, you can use the command-line interface version of NetExtender.

Using Mobile Connect

SonicWall Mobile Connect serves the same function as NetExtender on iOS, Android, Mac OS X, Windows Phone, Windows 10, and ChromeOS. Mobile Connect is an app that, like NetExtender, uses SSL VPN to enable secure, mobile connections to private networks protected by SonicWall security appliances. For information about installing and using SonicWall Mobile Connect, see the *SonicWall Mobile Connect User* documentation for your device at:
https://support.sonicwall.com/sonicwall-secure-mobile-access/sma%206200/release-notes-guides.

Mobile Connect is compatible with Secure Mobile Access and is a free download from the app store for the type of device.

Mobile Connect acts as a NetExtender client when connecting to Secure Mobile Access. For Mobile Connect access to succeed, the portal must be set to allow NetExtender connections and the user account and group must be authorized to use NetExtender.

Prerequisites for Apple iOS clients

Mobile Connect is supported on Apple iPhone, iPad, and iPod Touch devices running Apple iOS. For a list of specific supported devices, see the *SonicWall Mobile Connect iOS User* documentation.

- For Mobile Connect 3.1, iOS 6 or higher is required on the device.
- For Mobile Connect 4.0, iOS 7 or higher is required on the device.

Prerequisites for Android Smartphone clients

The SonicWall Mobile Connect app can be used for smartphones running Android:

- For Mobile Connect 3.1, Android 4.0 or higher is required on the device.
- For Mobile Connect 4.0, Android 4.1 or higher is required on the device.

User configuration tasks

SonicWall NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

The following sections describe how to use NetExtender on the various supported platforms:

Windows Platform Installation

- Installing NetExtender using the Mozilla Firefox browser on page 33
- Installing NetExtender using the Internet Explorer browser on page 35
- Installing NetExtender Using the Chrome Browser on page 37

Windows Platform Usage

- Launching NetExtender Directly from Your Computer on page 40
- Configuring NetExtender Properties on page 42
- Configuring NetExtender Connection Scripts on page 44
- Configuring Batch File Commands on page 44
- Configuring Proxy Settings on page 45
- Configuring NetExtender Log Properties on page 47
- Configuring NetExtender Advanced Properties on page 48
- Configuring NetExtender Acceleration Properties on page 49
- Configuring NetExtender Packet Capture Properties on page 49
- Configuring Language Properties on page 50
- Viewing the NetExtender Log on page 51
- Disconnecting NetExtender on page 51
- Upgrading NetExtender on page 52
- Changing Passwords on page 52
- Authentication Methods on page 52
- Uninstalling NetExtender on page 53
- Verifying NetExtender operation from the System Tray on page 53
- Using the NetExtender Command Line Interface on page 54

Linux Platform

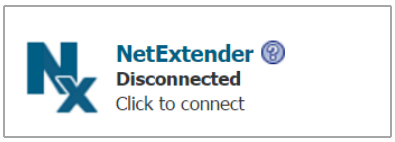
- Installing NetExtender on Linux on page 55
- Using NetExtender on Linux on page 57

Installing NetExtender using the Mozilla Firefox browser

To install NetExtender for the first time using the Firefox browser:

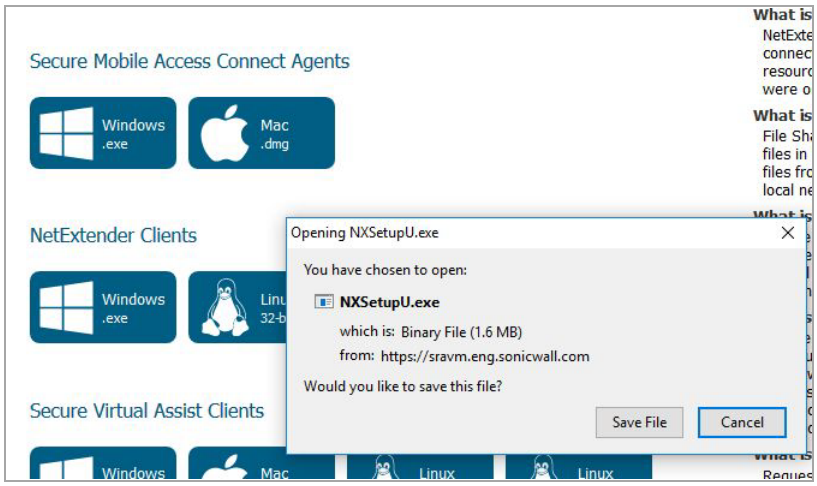
1 Log in to the Secure Mobile Access Virtual Office portal.

2 Click **NetExtender**.



3 The Client Download window pops up, with instructions for downloading and installing the NetExtender client. The instructions are:

> The client is downloaded automatically. If the download does not start automatically, select your platform for manual download.
>
> To install the client after download, run the application and follow the instructions from the installer.



4 The automatic download causes the **Opening NXSetupU.exe** dialog box to display. Click **Save File** to allow the NetExtender client to be downloaded to your computer. The file is saved in your Downloads folder.

5 Navigate to your Downloads folder and double-click **NXSetupU.exe** to run the installer.

6 The User Account Control dialog displays. Click **Yes** in answer to the question, “Do you want to allow the following program to make changes to this computer?”

7 The SonicWall NetExtender Setup wizard is launched. The Welcome screen recommends that you close all other applications before starting the setup to avoid the need to restart your computer after the installation. When ready to proceed, click **Next**.

8 In the License Agreement screen, read the agreement, select **I accept the terms of the License Agreement** and then click **Next**.

9 In the Choose Install Location screen, optionally change the **Destination Folder** field by using **Browse**. Click **Next**.

10 In the Shortcuts screen, the following shortcut options are selected by default:

- Create a shortcut on StartMenu.

- Create a shortcut on QuickLaunch bar.
- Create a shortcut on Desktop

Clear the check boxes for any of these shortcut options that you do not want.

11 Click **Install**.

12 If a Windows Security dialog box asks, “Would you like to install this device software?”, click **Install**.

13 In the Completing the SonicWall NetExtender Setup Wizard screen, leave the **Run SonicWall NetExtender** check box selected to launch NetExtender immediately, or clear the check box to complete the installation without launching NetExtender.

14 Click **Finish**.

15 If NetExtender is launched, type the IP address or FQDN of the SMA/SRA appliance into the **Server** field. This is the same server that you point your browser to when accessing the portal page to download NetExtender.

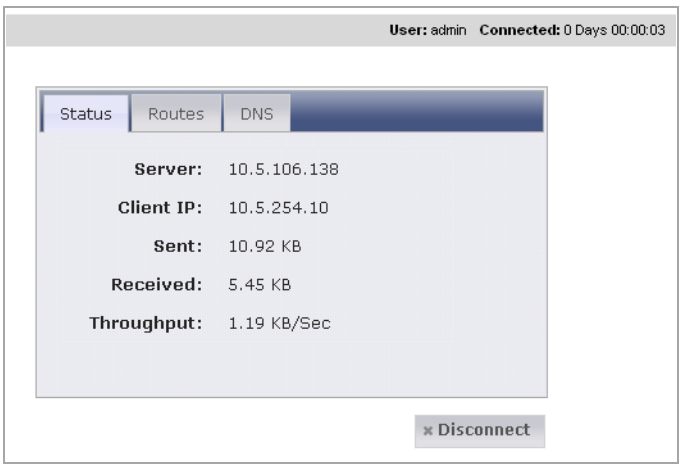
16 In the **Username** field, type in your user name.

17 In the **Password** field, type in your password.

18 In the **Domain** field, type in the domain. This is the same domain shown in the **Domain** field of the login page when you access the portal in your browser.

19 Click **Connect**. NetExtender takes a few seconds to connect to the server and verify your credentials.

The **NetExtender** status window displays, indicating that NetExtender successfully connected. The NetExtender icon is displayed in the task bar.



The **Status** tab provides the following information:

Status tab field descriptions

Field	Description
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Throughput	Indicates the current NetExtender throughput rate.

TIP: Closing the window (clicking the x icon in the upper right corner of the window) does not close the NetExtender session, but minimizes it to the system tray for continued operation.

20 To disconnect NetExtender, click **Disconnect**.

Installing NetExtender using the Internet Explorer browser

Secure Mobile Access NetExtender is fully compatible with Microsoft Windows 7 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems. NetExtender is also compatible with the Mac OS X Lion 10.7.

NOTE: It might be necessary to restart your computer when installing NetExtender on Windows 7.

Internet Explorer Prerequisites

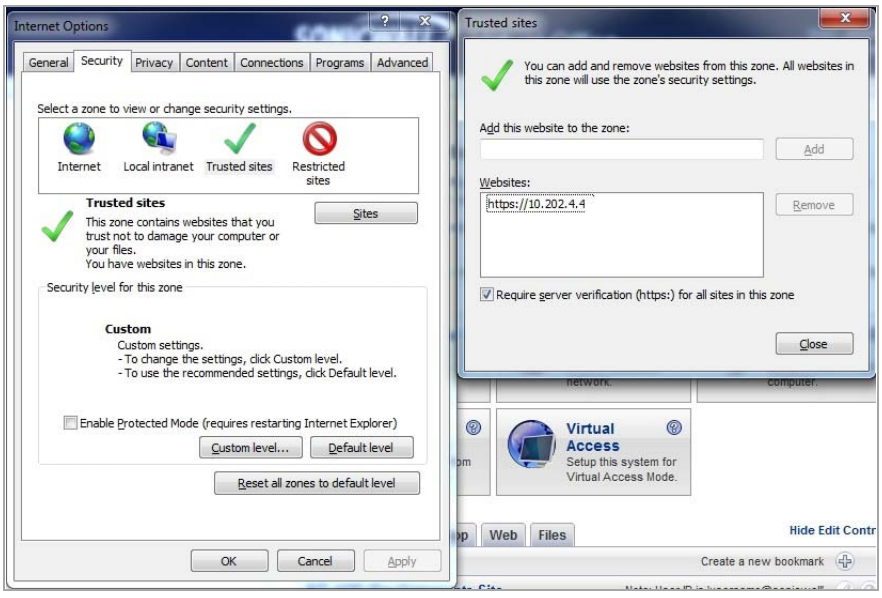
It is recommended that you add the URL or domain name of your SMA/SRA server to Internet Explorer's trusted sites list. This simplifies the process of installing NetExtender and logging in, by reducing the number of security warnings you receive.

To add a site to Internet Explorer's trusted sites list:

1 In Internet Explorer, go to **Tools > Internet Options**.

2 Click the **Security** tab.

3 Click **Trusted Sites** and click **Sites...** to open the **Trusted sites** window.



4 Enter the URL or domain name of your SMA/SRA server in the **Add this Web site to the zone** field and click **Add**.

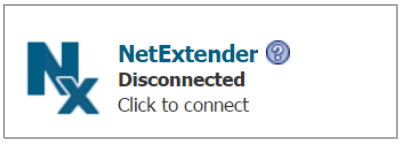
5 Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Internet Explorer browser:

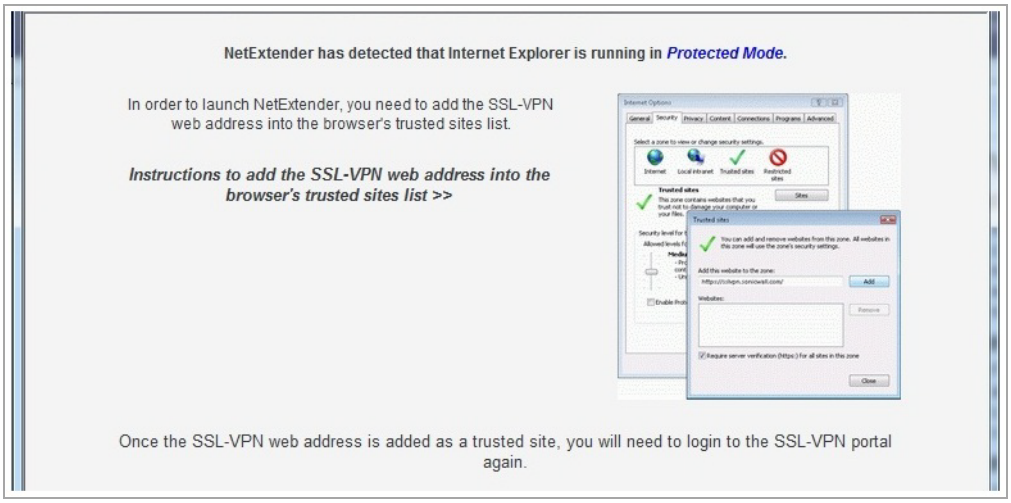
1 Log in to the Secure Mobile Access Virtual Office portal.

2 Click **NetExtender**.



3 A User Account Control window can appear asking “Do you want to allow this program to make changes to this computer?” Click **Yes**.

4 The first time you launch NetExtender, you must first add the Secure Mobile Access portal to your list of trusted sites. If you have not done so, the follow message displays.

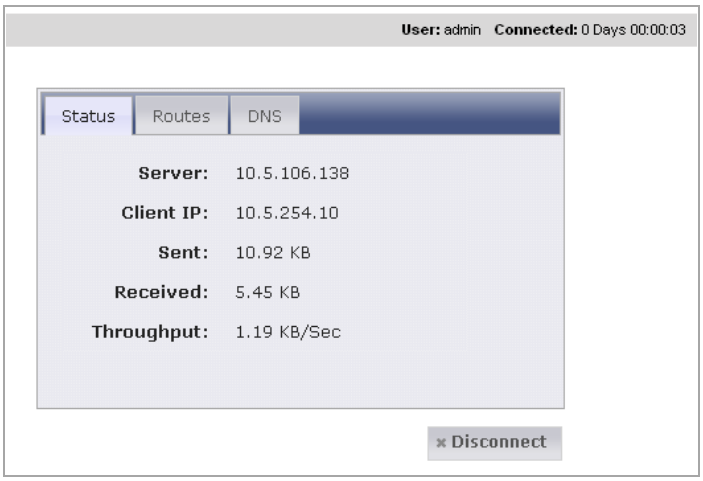


5 For details on how to add the Virtual Office as a trusted site, see the Internet Explorer Prerequisites on page 35.

6 Return to the Secure Mobile Access portal and click **NetExtender**. The portal automatically installs the NetExtender standalone application on the computer, and the NetExtender installer opens.

If an older version of NetExtender is installed on the computer, the NetExtender launcher removes the old version and then installs the new version.

7 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender has successfully connected.



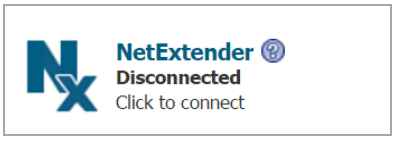
The information provided in the NetExtender Status window is described in the Status tab field descriptions table in Installing NetExtender using the Mozilla Firefox browser on page 33.

Installing NetExtender Using the Chrome Browser

To install and launch NetExtender for the first time using the Chrome browser:

1 Log in to the Secure Mobile Access Virtual Office portal.

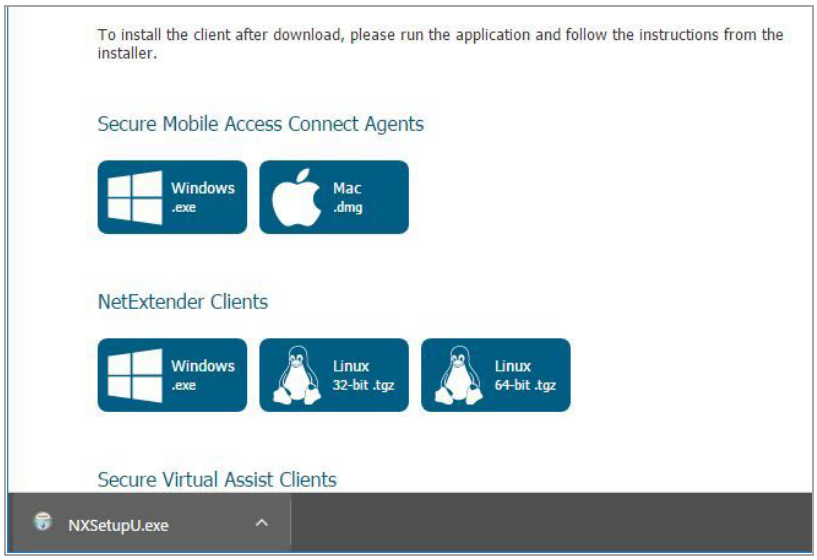
2 Click **NetExtender**.



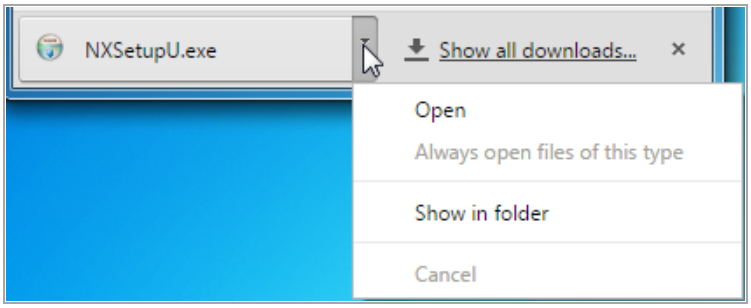
3 The Client Download window pops up, with instructions for downloading and installing the NetExtender client. The instructions are:

> The client is downloaded automatically. If the download does not start automatically, select your platform for manual download.

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



4 The automatic download causes the **NXSetupU.exe** file to show at the bottom of the window. Click the small arrow to see the available actions.



5 Click **Open** to launch the NetExtender installer, or click **Show in Folder** to view the file in your Downloads folder. If you select **Show in Folder**, double-click **NXSetupU.exe there** to run the installer.

6 The User Account Control dialog displays. Click **Yes** in answer to the question, “Do you want to allow the following program to make changes to this computer?”

7 The SonicWall NetExtender Setup wizard is launched. The Welcome screen recommends that you close all other applications before starting the setup to avoid the need to restart your computer after the installation. This is optional, and a system restart might or might not be needed if you don’t close everything first. When ready to proceed, click **Next**.

8 In the License Agreement screen, read the agreement, select **I accept the terms of the License Agreement** and then click **Next**.

9 In the Choose Install Location screen, optionally change the **Destination Folder** field by using **Browse**. Click **Next**.

10 In the Shortcuts screen, the following shortcut options are selected by default:

- Create a shortcut on StartMenu.
- Create a shortcut on QuickLaunch bar.
- Create a shortcut on Desktop

11 Clear the check boxes for any of these shortcut options that you do not want.

12 Click **Install**.

13 If a Windows Security dialog box asks, “Would you like to install this device software?”, click **Install**.

14 In the Completing the SonicWall NetExtender Setup Wizard screen, leave the **Run SonicWall NetExtender** check box selected to launch NetExtender immediately, or clear the check box to complete the installation without launching NetExtender.

15 Click **Finish**.

16 If NetExtender is launched, type the IP address or FQDN of the SMA/SRA appliance into the **Server** field. This is the same server that you point your browser to when accessing the portal page to download NetExtender.

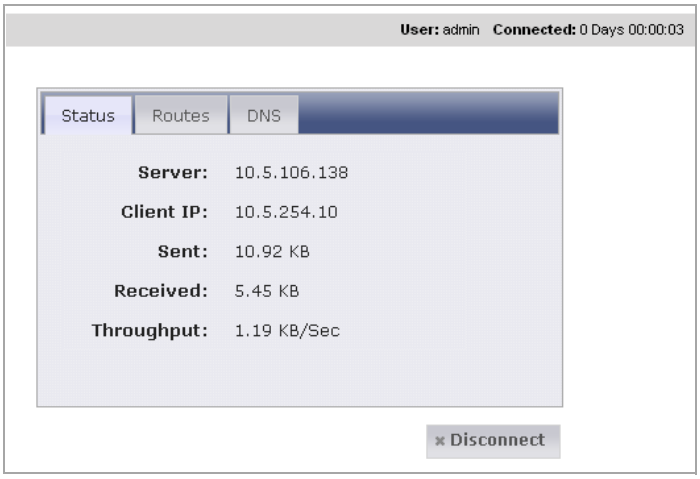
17 In the **Username** field, type in your user name.

18 In the **Password** field, type in your password.

19 In the **Domain** field, type in the domain. This is the same domain shown in the **Domain** field of the login page when you access the portal in your browser.

20 Click **Connect**. NetExtender takes a few seconds to connect to the server and verify your credentials.

The **NetExtender** status window displays, indicating that NetExtender successfully connected. The NetExtender icon is displayed in the task bar.



The **Status** tab provides the following information:

Status tab field descriptions

Field	Description
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Throughput	Indicates the current NetExtender throughput rate.

TIP: Closing the window (clicking the x icon in the upper right corner of the window) does not close the NetExtender session, but minimizes it to the system tray for continued operation.

Launching NetExtender Directly from Your Computer

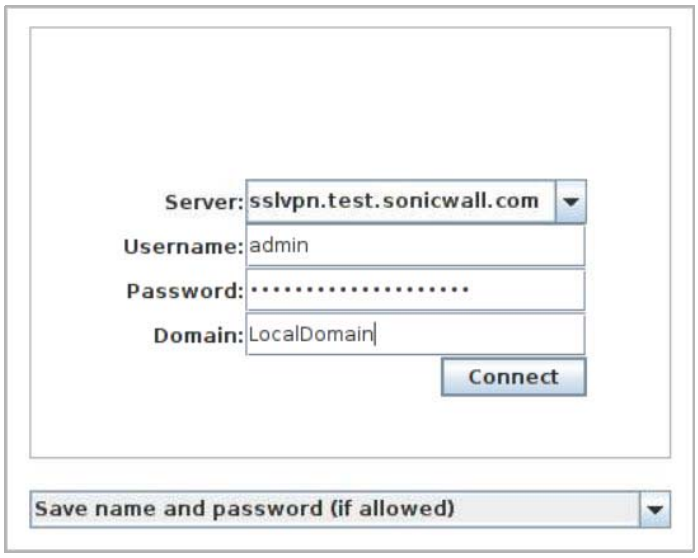
After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the Secure Mobile Access portal.

To launch NetExtender:

1 Navigate to **Start > All Programs**.

2 Select the **SonicWall NetExtender** folder, and then click **SonicWall NetExtender**. The NetExtender login window is displayed.

3 The IP address of the last SMA/SRA server you connected to is displayed in the **Server** field. To display a list of recent SMA/SRA servers you have connected to, click the arrow.



4 Enter your username and password.

5 The last domain you connected to is displayed in the **Domain** field.

NOTE: The NetExtender client reports an error message if the provided domain is invalid when you attempt to connect. Keep in mind that domain names are case-sensitive.

6 The drop-down menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

TIP: Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

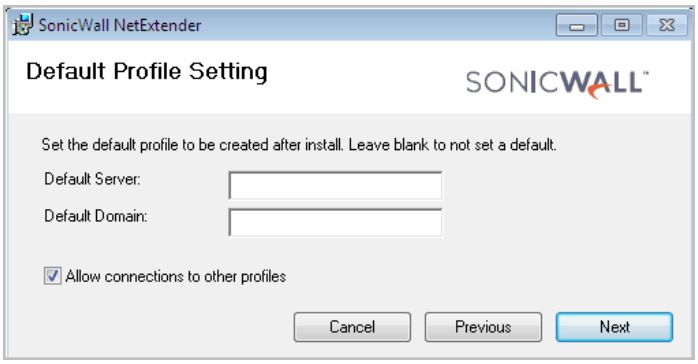
Pre-filling the Server and Domain Fields while Installing NetExtender through Microsoft Installer

Installing NetExtender through Microsoft Installer (MSI) now supports the use of default profile settings during the installation process where the default server and default domain can be pre-filled along with additional options that control whether the server and domain fields can be edited by a standard user. This feature is

designed specifically for administrators who want their default servers and domains pre-set during the installation process.

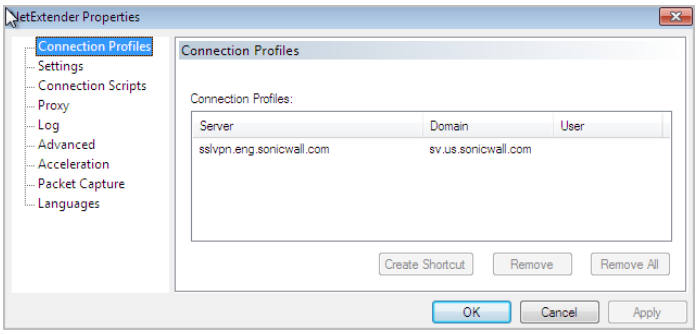
To set the default server and domain during the NetExtender Installation with Microsoft Installer,

1 On the **Default Profile Setting** page, enter the IP address of the **Default Server** in the appropriate field and the location of the **Default Domain** in the second field.



2 Disable **Allow connections to other profiles** to prevent users from connecting to other profiles. This setting disables the Server and Domain fields for editing on the login page of NetExtender.

3 Enable this option to allow those connections. If this option is not enabled, users are not able to add or delete profiles on the NetExtender properties page.



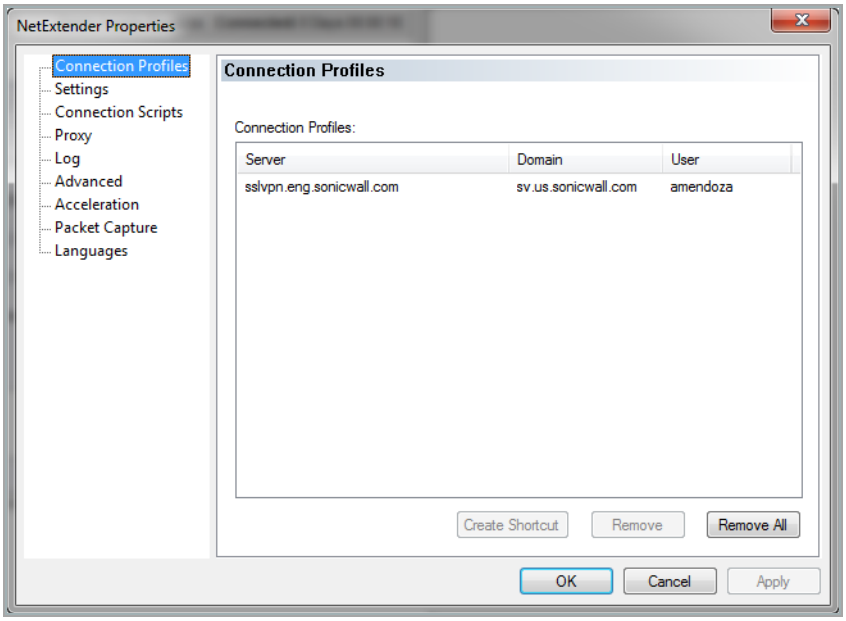
Configuring NetExtender Properties

To configure NetExtender properties:

1 Right click the icon in the system tray and click **Properties...** The NetExtender Properties window is displayed.

Connection Profiles tab

The **Connection Profiles** tab displays the Secure Mobile Access connection profiles you have used, including the IP address of the SMA//SRA server, the domain, and the username.



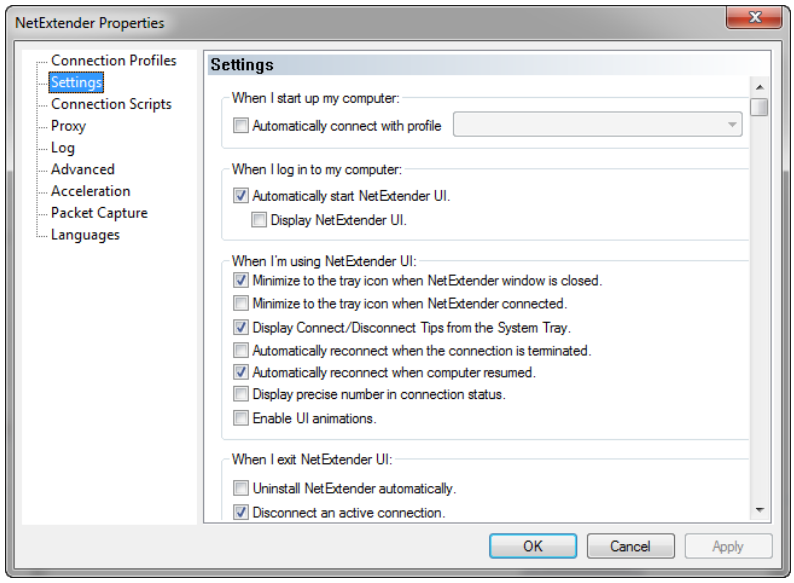
2 To create a shortcut on your desktop that launches NetExtender with the specified profile, highlight the profile and click **Create Shortcut**.

3 To delete a profile, highlight it by clicking on it and then click **Remove**. Click **Remove All** to delete all connection profiles.

4 Click **Apply** to save your changes.

Settings tab

The **Settings** tab allows you to customize the behavior of NetExtender.



5 To have NetExtender connect to a specific profile when starting up your computer, select **Automatically connect with profile** and select the profile from the drop-down list.

6 To have NetExtender launch when you log in to your computer, select the **Automatically start NetExtender UI**. NetExtender starts, but is only displayed in the system tray. To have the NetExtender login window display, select **Display NetExtender UI**.

7 Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not selected, you are only able to access the NetExtender UI through Window's program menu.

8 Select **Minimize to the tray icon when NetExtender connected** to have the NetExtender icon display in the system tray when you are connected.

9 Select **Display Connect/Disconnect Tips from the System Tray** to have NetExtender display tips when you mouse over the NetExtender icon.

10 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

11 Select **Automatically reconnect when computer resumed** to have NetExtender reconnect when the computer resumes from a sleep or a locked mode.

12 Select **Display precise number in connection status** to display precise byte value information in the connection status.

13 Select **Enable UI animations** to enable the sliding animation effects in the UI.

14 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

15 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session.

16 Select **Uninstall EPC Agent automatically** to have the End Point Control Agent uninstalled when NetExtender is uninstalled from the system.

17 Click **OK** to save your changes.

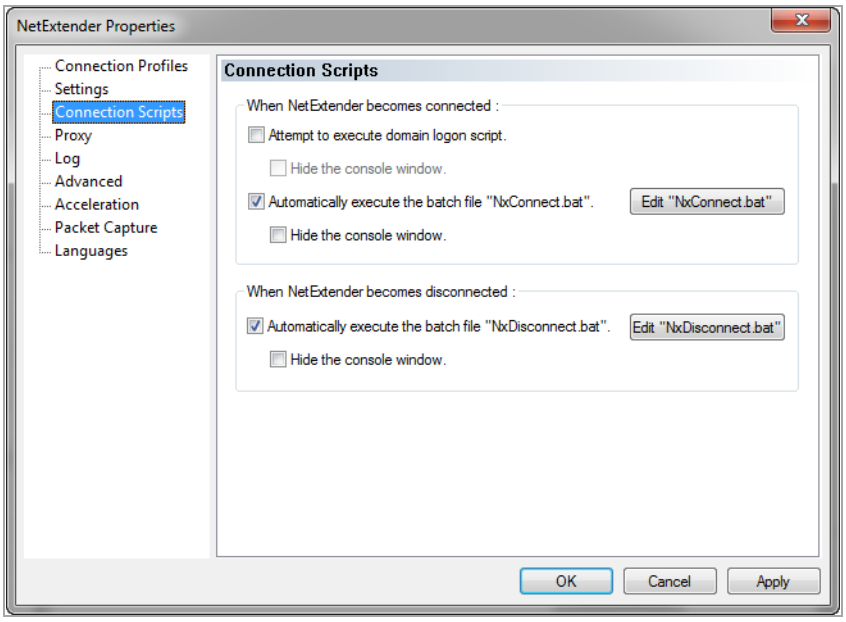
Configuring NetExtender Connection Scripts

Secure Mobile Access provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or web sites.

To configure NetExtender Connection Scripts:

1 Right click the icon in the task bar and click **Properties...** The NetExtender Preferences window is displayed.

2 Click **Connection Scripts**.



3 To enable the domain login script, select the **Attempt to execute domain logon script** check box. When enabled, NetExtender attempts to contact the domain controller and execute the login script. Optionally, you might now also select to **Hide the console window**. If this check box is not selected, the DOS console window remains open while the script runs.

> **NOTE:** Enabling this feature might cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible through NetExtender routes.

4 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** check box. Optionally, you can now also select to **Hide the console window**. If this check box is not selected, the DOS console window remains open while the script runs.

5 To enable the script that runs when NetExtender disconnects, select **Automatically execute the batch file "NxDisconnect.bat."**

6 Click **Apply** to save your changes.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

1 To configure the script that runs when NetExtender connects, click **Edit "NxConnect.bat."** The NxConnect.bat file is displayed.

2 To configure the script that runs when NetExtender disconnects, click **Edit "NxDisconnect.bat."** The NxConnect.bat file is displayed.

3 By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. Too add commands, scroll to the bottom of the file.

4 To map a network drive, enter a command in the following format:

```
net use drive-letter\\server\share password /user:Domain\name
```

For example to if the drive letter is z, the server name is engineering, the share is docs, the password is 1234, the user's domain is eng and the username is admin, the command would be the following:

```
net use z\\engineering\docs 1234 /user:eng\admin
```

5 To disconnect a network drive, enter a command in the following format:

```
net use drive-letter: /delete
```

For example, to disconnect network drive z, enter the following command:

```
net use z: /delete
```

6 To map a network printer, enter a command in the following format:

```
net use LPT1 \\ServerName\PrinterName /user:Domain\name
```

For example, if the server name is engineering, the printer name is color-print1, the domain name is eng, and the username is admin, the command would be the following:

```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```

7 To disconnect a network printer, enter a command in the following format:

```
net use LPT1 /delete
```

8 To launch an application enter a command in the following format:

```
C:\Path-to-Application\Application.exe
```

9 For example, to launch Microsoft Outlook, enter the following command:

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

10 To open a Web site in your default browser, enter a command in the following format:

```
start http://www.website.com
```

11 To open a file on your computer, enter a command in the following format:

```
C:\Path-to-file\myFile.doc
```

12 When you have finished editing the scripts, save the file and close it.

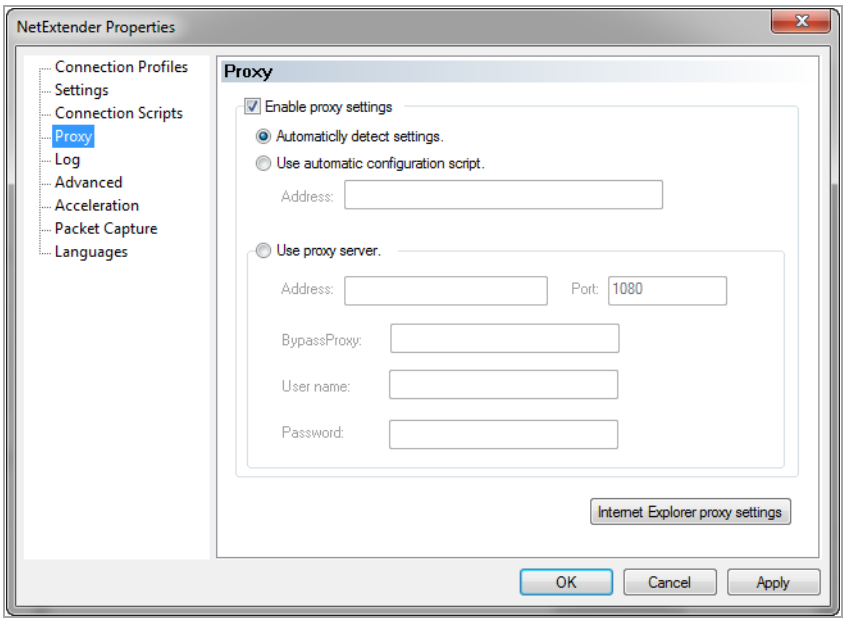
Configuring Proxy Settings

Secure Mobile Access supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings:

1 Right click the icon in the task bar and click **Preferences...** The NetExtender Preferences window is displayed.

2 Click **Proxy**.



3 Select **Enable proxy settings**.

4 NetExtender provides three options for configuring proxy settings:

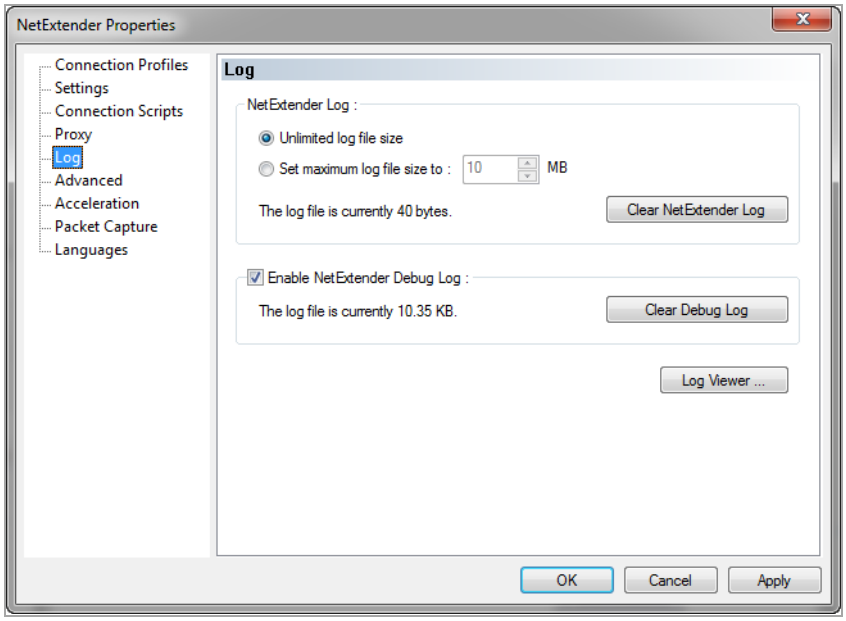
- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)) that can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Properties** window, a NetExtender pop-up window prompts you to enter them when you first connect.

5 Click **Internet Explorer proxy settings** to open Internet Explorer's proxy settings.

6 Click **Apply** to save your changes.

Configuring NetExtender Log Properties

Within the NetExtender Properties dialog box, click the Log heading in the menu on the left panel. The available options provide basic control over the NetExtender Log and Debug Log.



1 To establish the size of the NetExtender Log, select either **Unlimited log file size** or **Set maximum log file size to**. If you choose to set a maximum size, use the adjoining arrows. To clear the NetExtender Log, select **Clear NetExtender Log**.

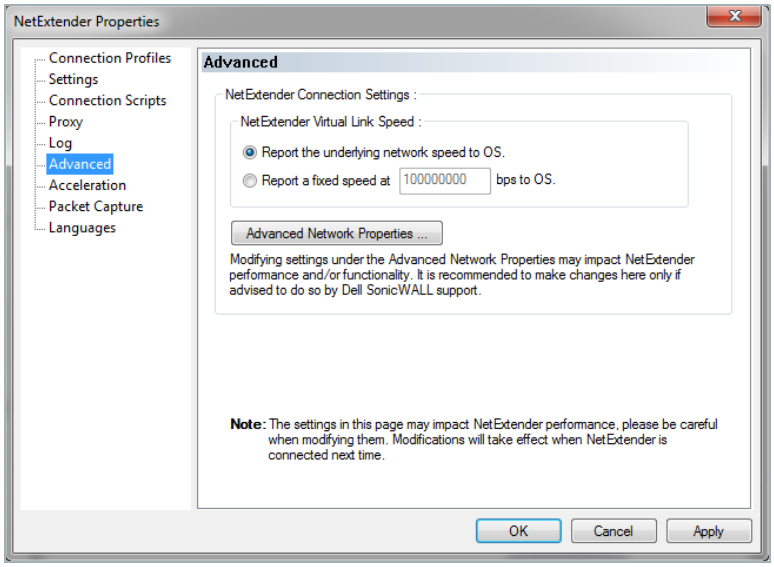
2 To **Enable the NetExtender Debug Log**, select the corresponding check box. To clear the debug log, select **Clear Debug Log**.

3 Click **Log Viewer...** to view the current NetExtender log.

4 Click **Apply** to save your changes.

Configuring NetExtender Advanced Properties

Within the NetExtender Properties dialog box, click the **Advanced** heading in the menu on the left panel. The available options allow you to adjust advanced settings on NetExtender network properties and protocols.



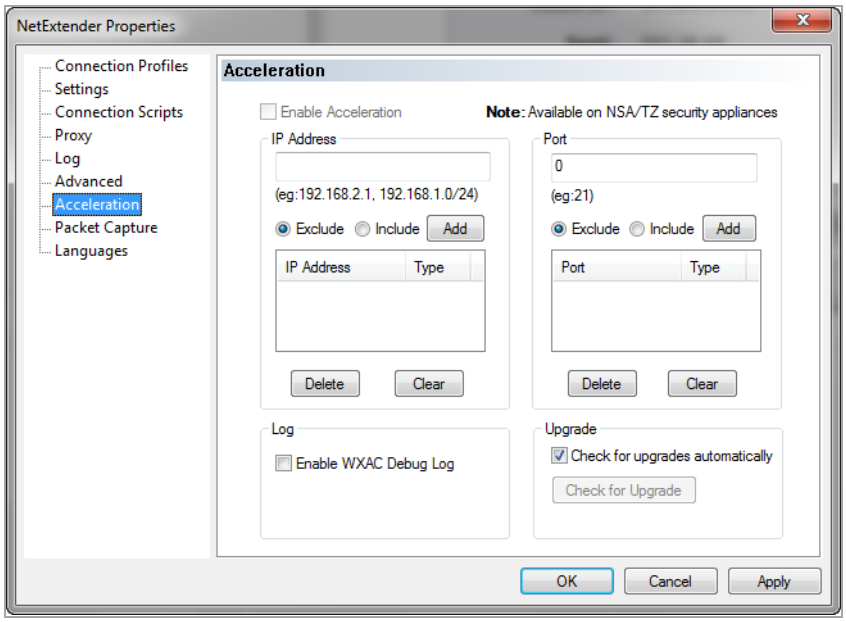
NetExtender allows users to customize the link speed that the NetExtender adapter reports to the operating system.

1 To select a virtual link speed to report, select either **Report the underlying network speed to OS**, or select **Report a fixed speed** and designate a speed.

> **NOTE:** Users can click **Advanced Network Properties** to make adjustments. However, modifying these settings could impact NetExtender performance and/or functionality. It is recommended to only make changes here if advised to do so by SonicWall support.

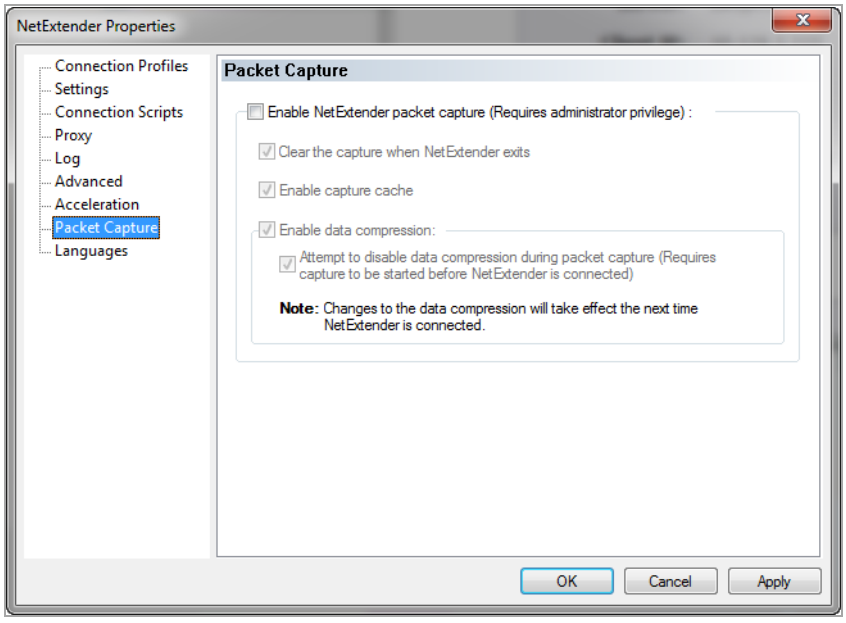
2 Click **OK** to save your changes.

Configuring NetExtender Acceleration Properties



Configuring NetExtender Packet Capture Properties

Within the NetExtender Properties dialog box, click the **Packet Capture** heading in the menu on the left panel. The available options allow you to enable and disable packet capture and data compression on NetExtender.



NOTE: You must have Administrator privileges to change packet capture settings.

To configure packet capture, complete the following steps:

1 To enable packet capture, select **Enable NetExtender packet capture**.

2 If packet capture is enabled, clear all captured packet data when NetExtender exits by selecting **Clear the capture when NetExtender exits**. To disable packet capture, clear this check box.

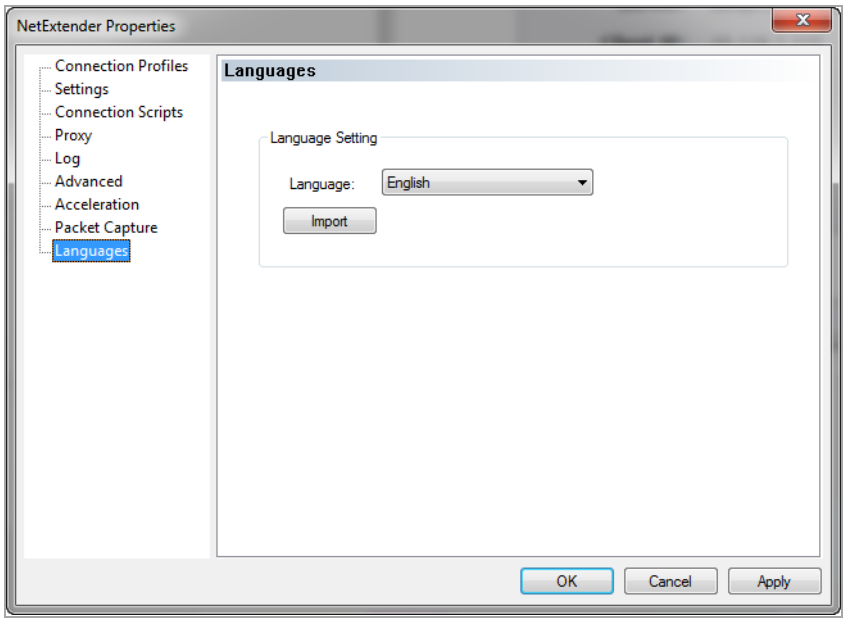
3 If packet capture is enabled, clear all captured packet data when NetExtender exits by selecting **Clear the capture when NetExtender exits**. To retain packet data, clear this check box.

4 To enable data compression of captured packets, select **Enable data compression**. To disable data compression the next time NetExtender is connected, clear this box. If packet capture is enabled when NetExtender connects and you want to disable data compression immediately (instead of waiting until the next time NetExtender is connected), select **Attempt to disable data compression during packet capture**.

5 Click **Apply** to save your changes.

Configuring Language Properties

Within the NetExtender Properties dialog box, click the **Languages** heading in the menu on the left panel. The available options allow you to select your language settings or import other language packs on NetExtender.



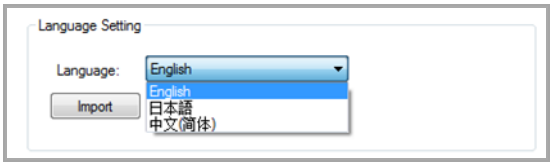
To configure language properties, complete the following steps:

1 The **Language** drop-down list allows you to select the available languages on NetExtender. The default language is English. After you select a language from the drop-down list, click **OK**. Restart NetExtender for the new language to be applied.

2 **Import** allows you to upload a new language pack to NetExtender. Click **Import**. Select the language pack you want to import. Click **Open**.

NOTE: Language packs must be in .ZIP format.

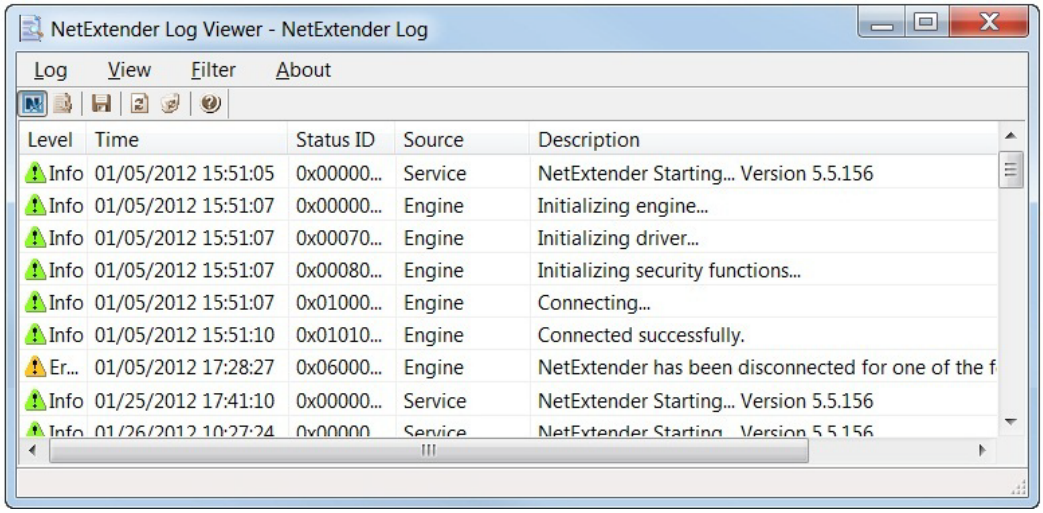
After the import, the language displays in the Language drop-down list.



3 Click **Apply** to save your changes.

Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory: `C:\Program Files\SonicWall\SSL VPN\NetExtender`. To view the NetExtender log, right click the NetExtender icon in the system tray, and click **View Log**, click the Log icon on the main status page.



To view details of a log message, double-click a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export**.

To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal, Error, Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all Error and Fatal entries, but not Warning or Info entries.

To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.

NOTE: It could take several minutes for the Debug Log to load. During this time, the Log window is not accessible, although you can open a new Log window while the Debug Log is loading.

To clear the log, click **Log > Clear Log**.

Disconnecting NetExtender

To disconnect NetExtender:

1 Right click the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.

2 Wait several seconds. The NetExtender session disconnects.

You can also disconnect by double-clicking on the **NetExtender** icon to open the NetExtender window and then clicking **Disconnect**.

When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

Upgrading NetExtender

NetExtender automatically notifies users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the SMA/SRA security appliance.

Changing Passwords

Before connecting to the new version of NetExtender, users might be required to reset their password by suppling their old password, along with providing and re-verifying a new one.

Authentication Methods

NetExtender supports various two factor authentication methods, including one-time password, RSA, and Vasco. If an Administrator has configured one-time passwords to be required to connect through NetExtender, you are asked to provide this information before connecting.

If an Administrator has configured RSA pin-mode authentication to be required to connect through NetExtender, users are asked whether they want to create their own pin, or receive one that is system-generated.

After the pin has been accepted, you must wait for the token to change before logging in to NetExtender with the new passcode.

During authentication, the SMA/SRA server can be configured by the Administrator to request a client certificate. In this case, users must select a client certificate to use when connecting.

Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click **Start > All Programs**, click **SonicWall NetExtender**, and then click **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected.

To configure NetExtender to automatically uninstall when your session is disconnected:

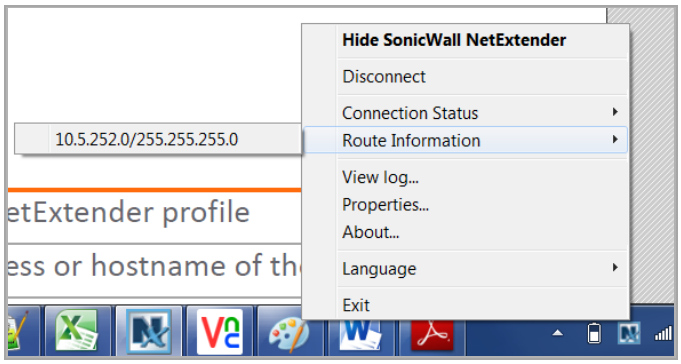
1. Right click the NetExtender icon in the system tray and click **Properties**... The **NetExtender Properties** window is displayed.
2. Click the **Settings** tab.
3. Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.
4. Click **Apply**.

Verifying NetExtender operation from the System Tray

To view options in the NetExtender system tray, right-click the NetExtender icon in the system tray. The following are some tasks you can complete with the system tray.

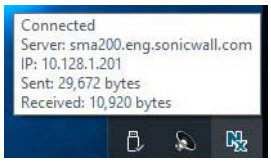
Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray.



Using the NetExtender Command Line Interface

NOTE: The NetExtender command line interface is only available on Windows platforms.

To launch the NetExtender CLI:

1. Launch the Windows Command Prompt by going to the **Start** menu, select **Run**, enter **cmd**, and click **OK**.
2. Change directory to where NetExtender is installed. To do this, you first must move up to the root drive by entering the **cd ..** command. Repeat this command until you are at the root drive. Then enter `cd Program Files\SonicWall\SSL-VPN\NetExtender`.

   NOTE: The specific command directory could be different on your computer. Use Windows Explorer to find the directory path where NetExtender is located.

Below, the NetExtender CLI commands and options table describes the commands available in the NetExtender CLI and their options.

NetExtender CLI commands and options

Command	Option	Description
NECLI addprofile		Creates a NetExtender profile
	-s *server*	The IP address or hostname of the SMA/SRA server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
NECLI connect		Initiates a NetExtender session.
	-s *server*	The IP address or hostname of the SMA/SRA server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
	- **clientcertificatethumb** *thumb*	The SSL Client Certificate thumbprint value.
	- **clientcertificatename** *name*	The SSL Client Certificate name.
NECLI deleteprofile		Deletes a saved NetExtender profile.
	-s *server*	The IP address or hostname of the SMA/SRA server.
	-u *user-name*	The username for the account.
	-d *domain-name*	The domain to connect to.

NetExtender CLI commands and options (Continued)

Command	Option	Description
NECLI disconnect		Disconnects
	timeout	(Optional) Timeout duration, after which the session is disconnected.
NECLI displayprofile		Displays all NetExtender profiles.
	-s *server*	(Optional) Displays only the profiles that are saved for the specified server.
	-u *user-name*	(Optional) Displays only the profiles that are saved for the specified user name.
	-d *domain-name*	(Optional) Displays only the profiles that are saved for the specified domain name.
NECLI queryproxy		Checks the connect to the proxy server.
NECLI reconnect		Attempts to reconnect to the server.
NECLI showstatus		Displays the status of the current NetExtender session.
NECLI setproxy		Configures proxy settings for NetExtender.
	-t [**0** |**1** | **2** | **3**]	There are three options for setting proxy settings: **0** - Disable proxy. **1** - Automatically detects proxy settings. The proxy server must support Web Proxy Auto Discovery Protocol (WPAD). **2** - Uses a proxy configuration script. **3** - Manually configure the proxy server.
	-s proxy address	The address of the proxy script or proxy server.
	-o port	The port number.
	-u user name	The user name for the proxy server.
	-p password	The password name for the proxy server.
	-b bypass-proxy	Bypasses the previously configured proxy settings.
	-save	Saves the proxy settings.
NECLI viewlog		Displays the NetExtender log.

Installing NetExtender on Linux

Secure Mobile Access supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

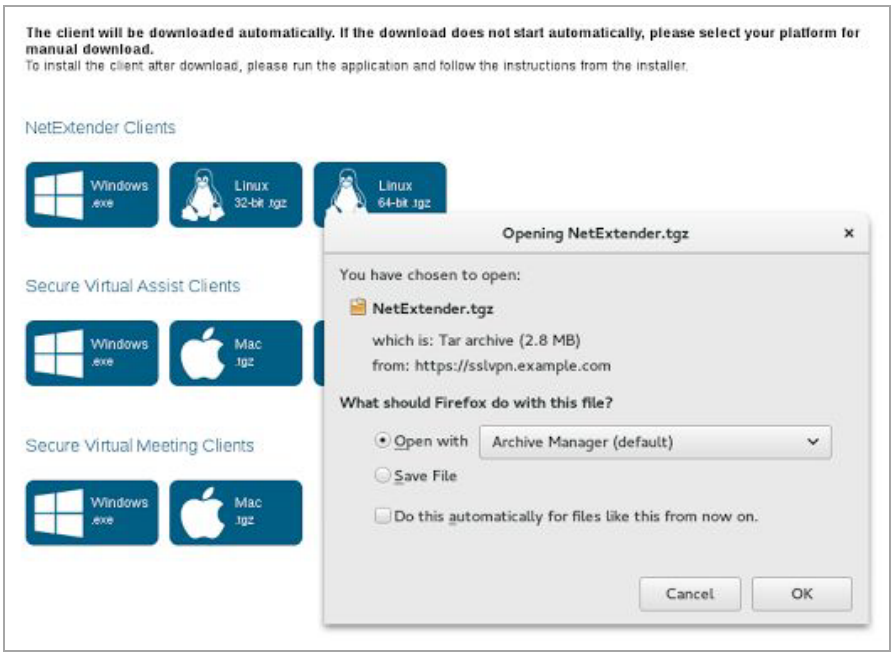
- i386-compatible distribution of Linux
- Linux Fedora Core 15 or higher, Ubuntu 11.10 or higher, or OpenSUSE 10.3 or higher
- Java 1.5 and higher is required for using the NetExtender GUI.

NOTE: Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5, you can use the command-line interface version of NetExtender.

To install NetExtender on your Linux system:

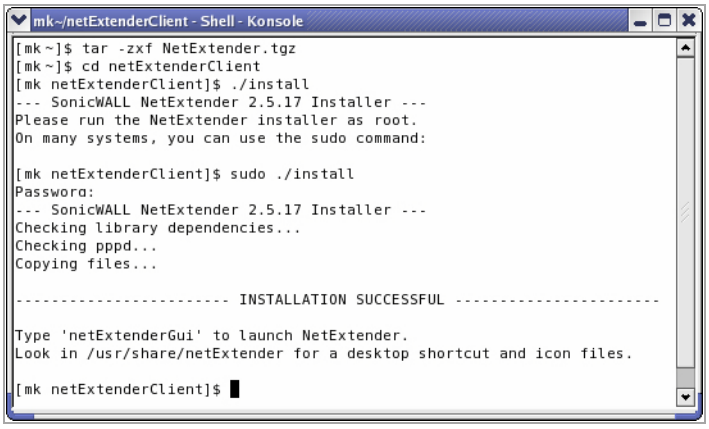
1 Log in to the SonicWall Virtual Office.

2 Click **NetExtender**. A pop-up window indicates that you have chosen to open a **.tgz** file. Click **OK** to save it to your default download directory.



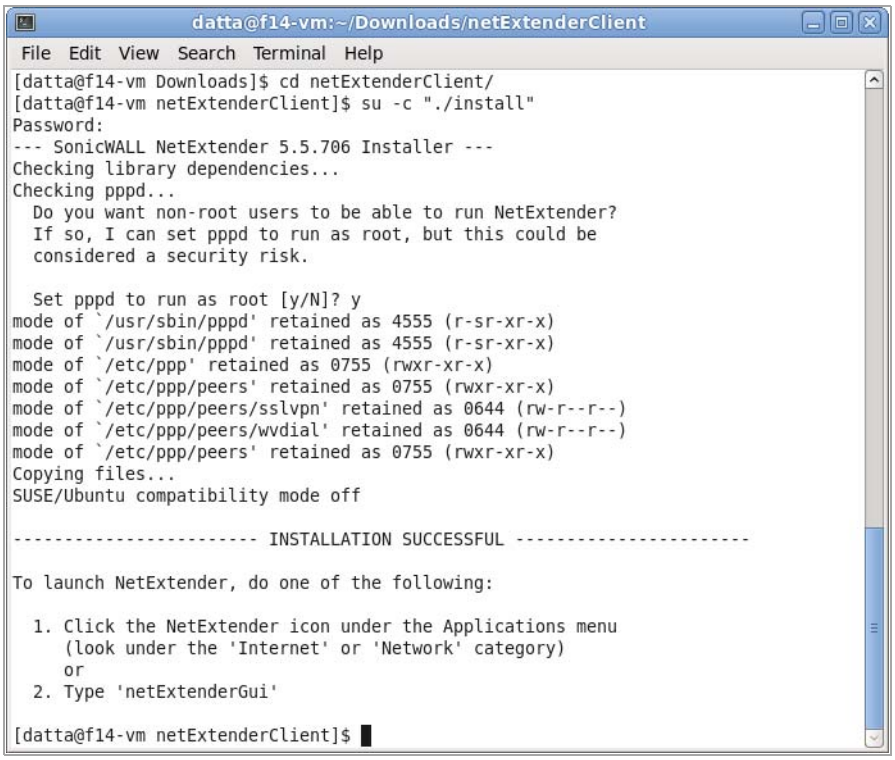
NOTE: You must be logged in as root to install NetExtender, although many Linux systems allows the **sudo ./install** command to be used if you are not logged in as root.

3 To install NetExtender from the CLI, navigate to the directory where you saved the **.tgz** file and enter the **tar -zxf NetExtender.tgz** command.



4 Enter the **cd netExtenderClient/** command.

5 Enter **su -C " ./install"** to install NetExtender.



6 Enter your system password.

7 The installer asks if you want non-root users to be able to run NetExtender. Enter either **y** for yes or **n** for no.

NOTE: To allow non-root users to run NetExtender, the installer sets PPPD to run as root. This could be considered a security risk.

Using NetExtender on Linux

To use NetExtender on a Linux computer:

1 After NetExtender is installed, there are two methods to launch it:

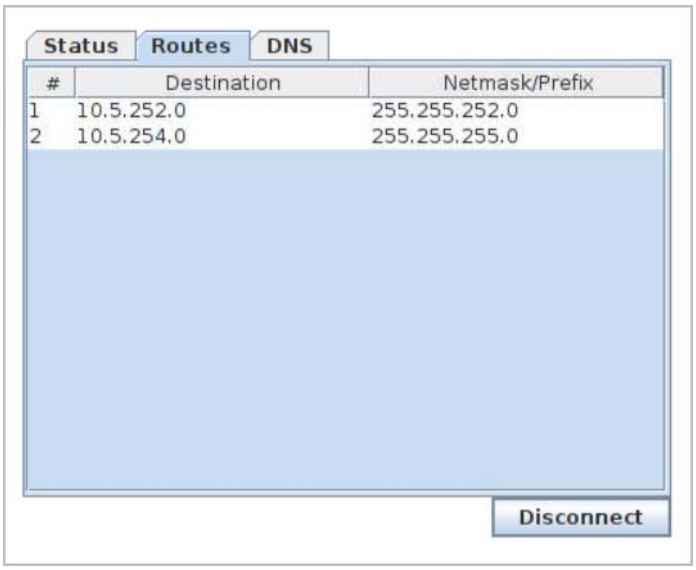
- Click the NetExtender icon in the Applications menu, under either the **Internet** or **Network** category.
- Enter the **netExtenderGui** command.

2 The first time you connect, you must enter the SMA/SRA server name in the **Server** field. NetExtender remembers the server name.

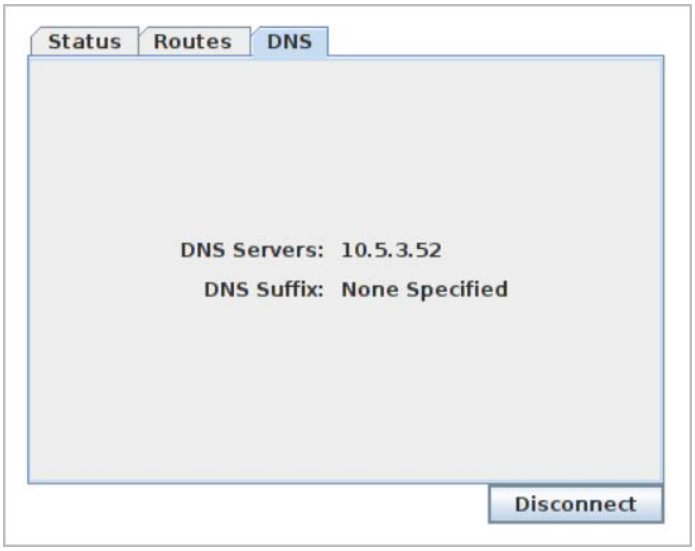
3 Enter your username and password.

4 The first time you connect, you must enter the **domain** name. The domain name is case-sensitive. NetExtender remembers the domain name in the future.

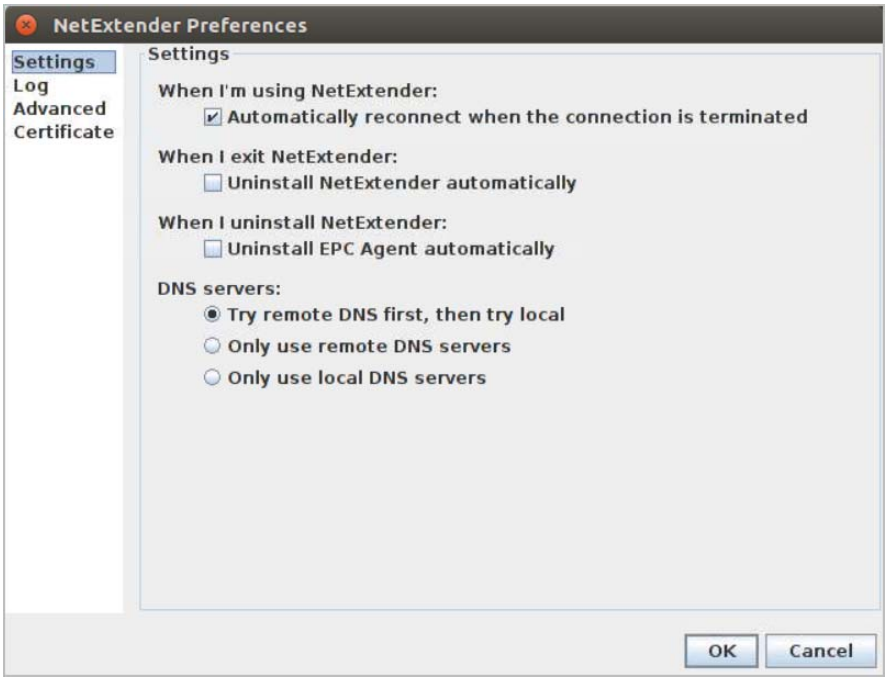
5 To view the NetExtender routes, select the **Routes** tab in the main NetExtender window.



6 To view the NetExtender DNS server information, select the **DNS** tab in the main NetExtender window.



7 To configure NetExtender Preferences, select **NetExtender > Preferences**.

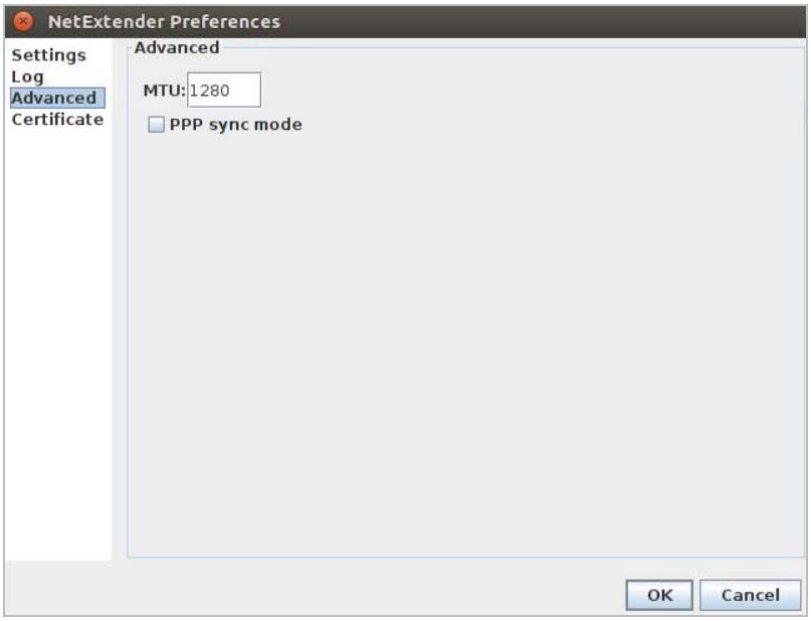


8 The following NetExtender settings can be configured:

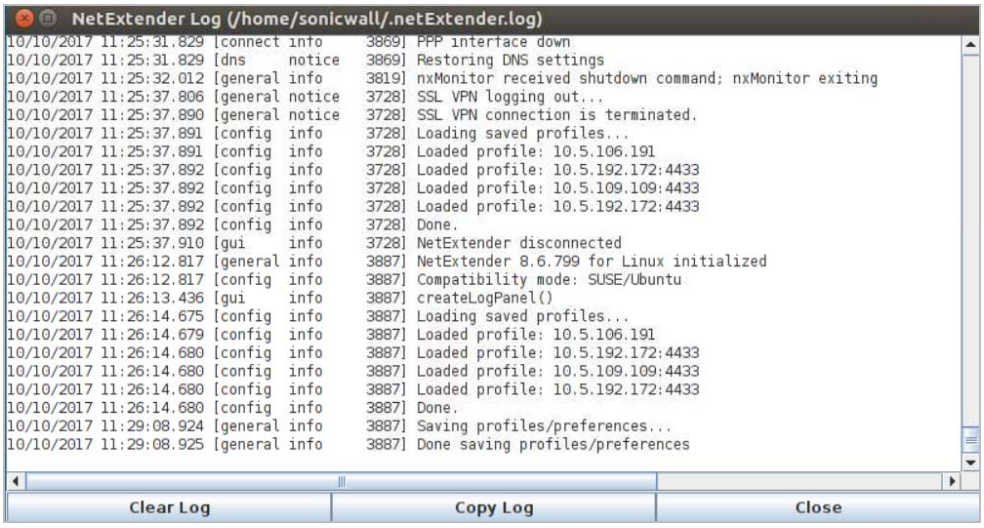
- Automatically reconnect when the connection is terminated
- Uninstall NetExtender automatically when exiting the application
- DNS server options:
  - Try remote DNS servers first, then try local DNS servers
  - Only use remote DNS servers
  - Only use local DNS servers

9 The Advanced tab of the NetExtender Preferences window provides two additional options:

- **MTU** - Sets the Maximum Transmission Unit (MTU) size that is the largest packet size that a router can forward without needing to fragment the packet.
- **PPP Sync Mode** - Specifies synchronous PPP. By default, this option is disabled and asynchronous PPP is used.



10 To view the NetExtender Log, go to **NetExtender > Log**.



11 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.

12 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

6

Using Secure Virtual Assist and Virtual Meeting

Secure Virtual Assist provides remote assistance and virtual meeting capabilities. Secure Virtual Assist is an easy to use tool that allows SonicWall Secure Mobile Access users to remotely support customers by taking control of their computers while the customer observes.

Secure Virtual Meeting allows Secure Mobile Access users to participate in virtual meetings through the Internet.

Topics:

- Using Secure Virtual Assist on page 61
- Using Secure Virtual Meeting on page 92

Using Secure Virtual Assist

The following sections describe how to use Secure Virtual Assist:

- Installing and Launching Secure Virtual Assist on page 62
- Configuring Secure Virtual Assist Settings on page 63
- Selecting a Secure Virtual Assist Mode on page 67
- Launching a Secure Virtual Assist Technician Session on page 68
- Performing Secure Virtual Assist Technician Tasks on page 70
- Initiating a Secure Virtual Assist Session from the Customer View on page 77
- Initiating Secure Virtual Assist on a Linux Client on page 84
- Using Secure Virtual Assist on page 85
- Using Secure Virtual Assist in Unattended Mode on page 87
- Using Virtual Access Mode on page 88
- Enabling a System for Secure Virtual Access on page 88
- Using the Request Assistance Feature on page 92

Secure Virtual Assist is a lightweight, thin client that installs automatically using the Secure Mobile Access Virtual Office. Secure Virtual Assist can also be installed as a standalone client that can be launched directly from the client's computer.

When a user requests service as a customer, Virtual Assist can be run while connected to the system over an RDP session for Windows 7 and Windows Vista platforms; however, Virtual Assist over RDP has a limited set of features.

There are two sides to a Virtual Assist session: the customer view and the Technician view. The customer is the person requesting assistance on their computer. The Technician is the person providing assistance. A Virtual Assist session consists of the following sequence of events:

1 The Technician launches Virtual Assist from the Secure Mobile Access Virtual Office.

2 The Technician monitors the Assistance Queue for customers requesting assistance.

3 The customer requests assistance by one of these methods:

- Logs into the Secure Mobile Access Virtual Office and clicks on the Request Assistance link.
- Receives an email invitation from the Technician and clicks on the link to launch Virtual Assist.
- Navigate directly to the URL of the Virtual Assist home page that is provided by the Technician.
- If the Virtual Assist client is already installed, launch the client and click the Request Assistance option.

4 The Secure Virtual Assist application installs and runs on the customer's system.

5 The customer appears in the Virtual Assist Assistance Queue.

6 The Technician clicks on the customers name and launches a Virtual Assist session.

7 The Technician's Virtual Assist window now displays the customers entire display. The Technician has complete control of the customer computer's mouse and keyboard. The customer sees all of the actions that the Technician does.

8 If at anytime the customer wants to end the session, they can take control and click **End Virtual Assist** in the bottom right corner of the screen.

9 When the session ends, the customer resumes sole control of the computer.

Installing and Launching Secure Virtual Assist

To install and launch a Virtual Assist session:

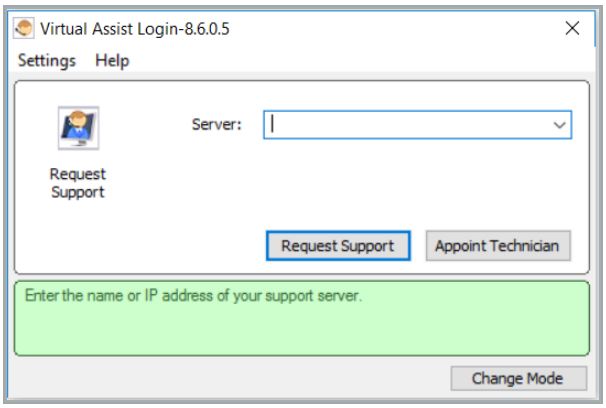
1 Log in to the Secure Mobile Access Virtual Office. If you are already logged in to the Secure Mobile Access customer interface, click **Virtual Office**.

2 Click **Request Assistance**.

3 The first time you launch Virtual Assist, you are prompted to install the Secure Virtual Assist plugin and client.

4 Click **Allow**. A plugin installation window displays. Click **Install Now**. The Secure Virtual Assist plugin and client installs. You might be prompted to restart your browser.

5 You can now launch Virtual Assist either from the Virtual Office window or from a shortcut that is added to your Programs list under Window's **Start** button.



Configuring Secure Virtual Assist Settings

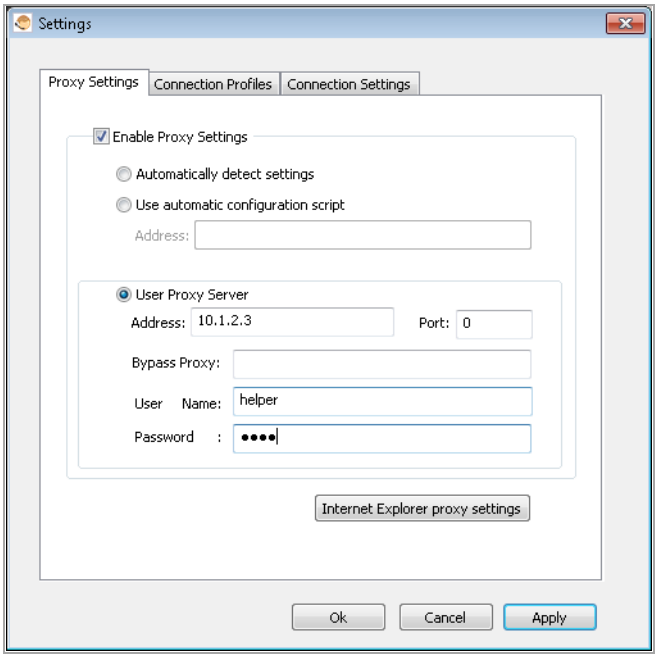
The Secure Virtual Assist Settings window can be accessed either by clicking **Settings** in the top left corner of the application window or by right-clicking on the Virtual Assist icon in the taskbar and selecting **Settings**. The Virtual Assist Settings window has three tabs. The content of these tabs and configuration vary depending on whether Secure Virtual Assist is being configured on a Windows or Mac OS X device.

- Windows Configuration on page 63
- Mac OS X Configuration on page 66
- Linux Configuration on page 67

Windows Configuration

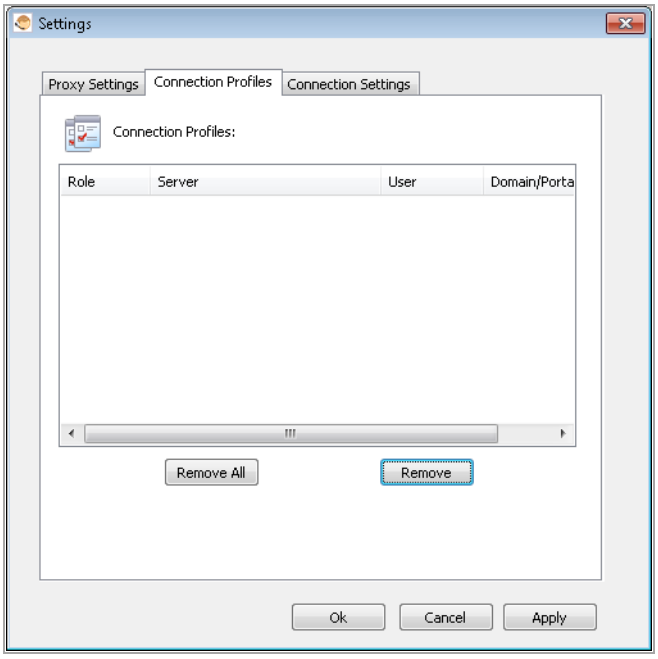
To configure Secure Virtual Assist for Windows:

- **Proxy Settings** - Allows users to configure a Proxy server to access the SMA/SRA appliance. There are three options for configuring proxy settings.

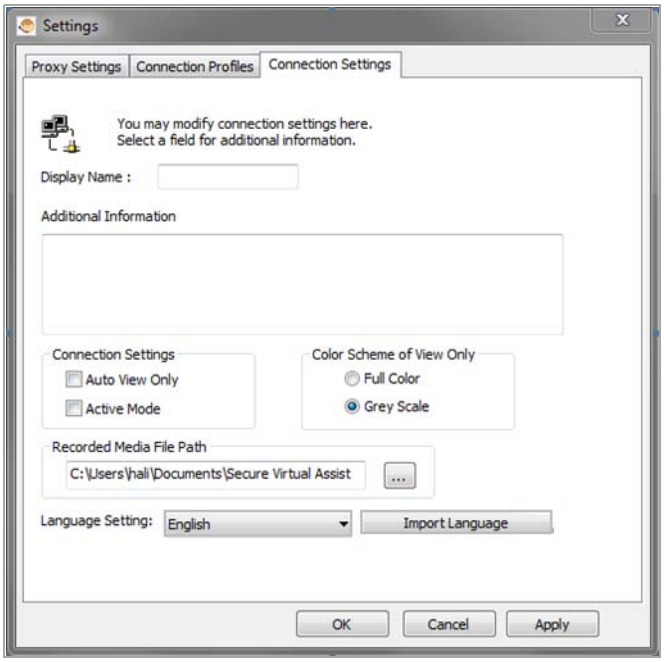


- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)) that can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Properties** window, a NetExtender pop-up window prompts you to enter them when you first connect.
- Optionally, you can click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings page.

- **Connection Profiles** - Displays all of the Virtual Assist connection profiles that have been used on this computer. To remove a profile, select it and click **Remove**.



- **Connection Settings** - Allows users to customize how they are identified in Virtual Assist and the default settings of Virtual Assist customer sessions.



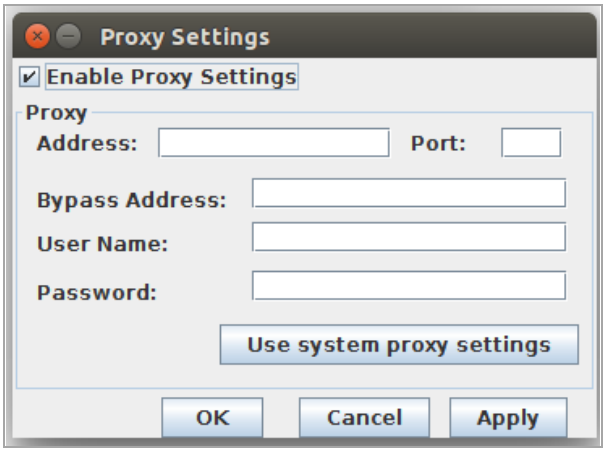
  - **Display Name** - The name that is displayed in the user queue. By default, the user account username is displayed.
  - **Additional Information** - Optional field to provide additional information.
  - **Auto View Only** - Specifies that Virtual Assist sessions initially launches in View-Only mode instead of Trusted mode, which is the default.
  - **Active Mode** - Specifies that Virtual Assist sessions initially launches in Active mode instead of Trusted mode, which is the default.
  - **Recorded Medial File Path** - The default location where the recorded support sessions are stored on the client PC.

- **Language Setting** - You can import language packages to have Virtual Assist display in languages other than the default (English). All language packages must be in .zip format.

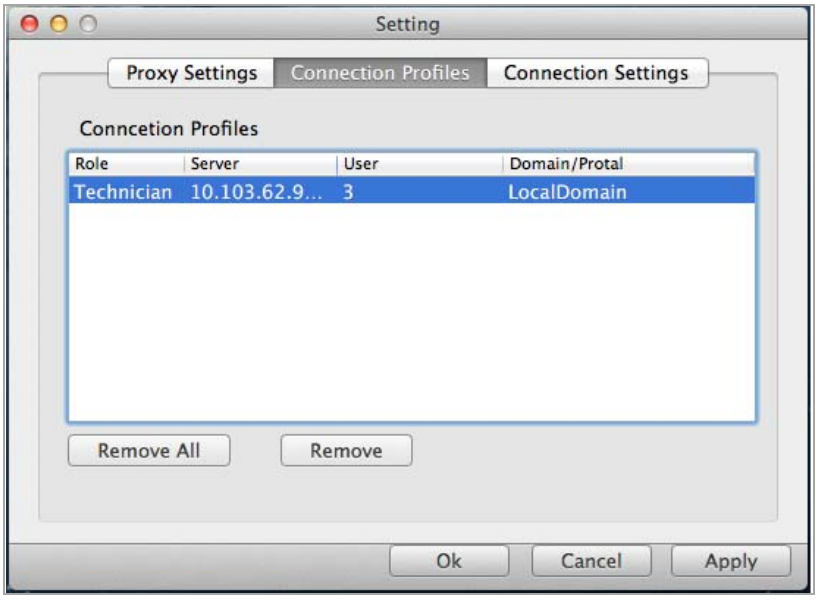
Mac OS X Configuration

To configure Secure Virtual Assist for Mac OS X:

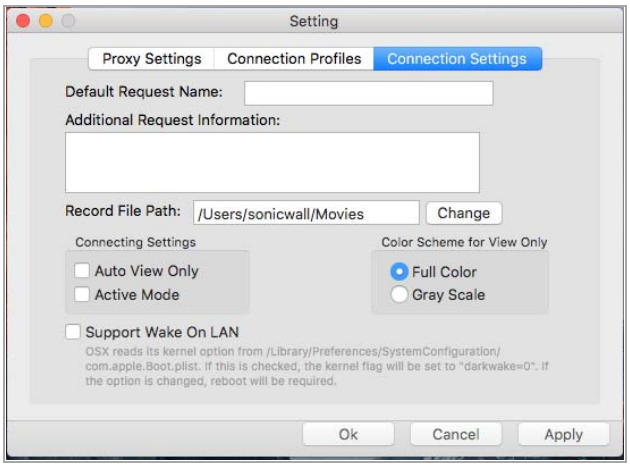
- **Proxy Settings** - Either load proxy settings from the system configuration by clicking **Load System Proxy Settings** or manually configure the proxy server, port, bypassed proxy, user name, and password.



- **Connection Profiles** - View and manage connection profiles in the Connection Profiles tab by clicking **Remove All** to remove all profiles or selecting the profile and clicking **Remove**.



6 **Connection Settings** - Create and edit connection profiles as follows:



- **Default Request Name** - Type the support request name for the customer.
- **Additional Request Information** - Type the support request information for the customer.
- **Connect Settings** - Select either Auto View Only or Active Mode. When **Auto View Only** is enabled, any mouse or keyboard action while a technician is connected triggers the View Only mode. When **Active Mode** is enabled, users are in Active mode by default while a technician is connected.
- **Color Scheme for View Only** - Select Full Color or Gray Scale. When **Full Color** is selected and the user is in View Only mode, the technician view is in full color. When **Gray Scale** is selected, the view is grey monochrome.

The Mac OS X Secure Virtual Assist windows and toolbar are very similar to the Windows version. Any significant differences are noted elsewhere in this document.

Linux Configuration

To configure Secure Virtual Assist for Linux:

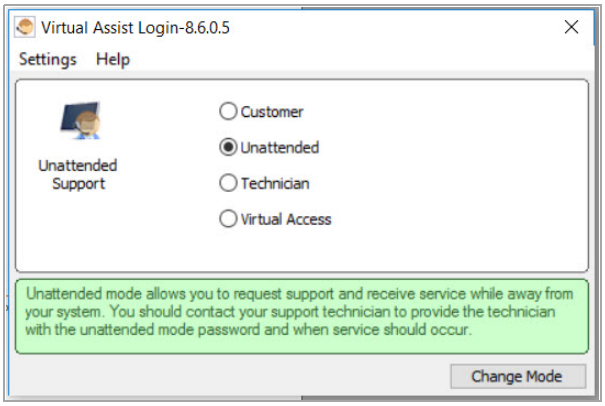
- **Proxy Settings** - Allows users to configure a Proxy server to access the SMA/SRA appliance. There are three options for configuring proxy settings.

Selecting a Secure Virtual Assist Mode

When you first launch Secure Virtual Assist, by default, it is in customer mode.

To change the mode:

1 Click **Change Mode** to select one of four possible modes.



2 Select one of the following four Virtual Assist modes:

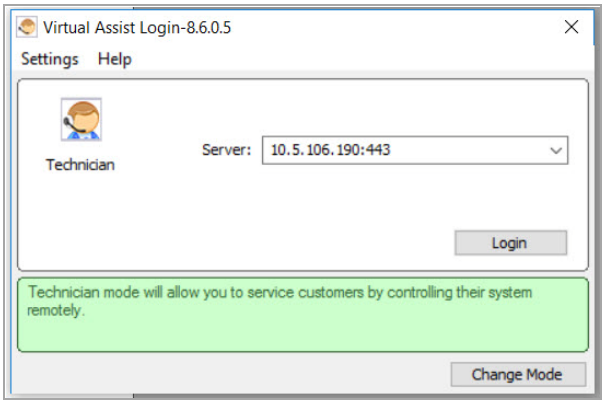
- **Customer** - Select this mode to request support. For information on customer mode, see Initiating a Secure Virtual Assist Session from the Customer View on page 77.
- **Unattended** - Select this mode to receive support help while you are away from your computer. You are prompted to enter a password that the Technician can then enter and assume control of your system without further confirmation from you. For information on unattended mode, see Using Secure Virtual Assist in Unattended Mode on page 87.
- **Technician** - Select this mode to service customers by remotely controlling their systems. For information on Technician mode, see Launching a Secure Virtual Assist Technician Session on page 68.
- **Virtual Access** - Select this mode to make your computer remotely accessible at all times from the SMA/SRA appliance. For information on Secure Virtual Access mode, see Enabling a System for Secure Virtual Access on page 88.

3 Click **Change Mode** again to login with the selected mode.

Launching a Secure Virtual Assist Technician Session

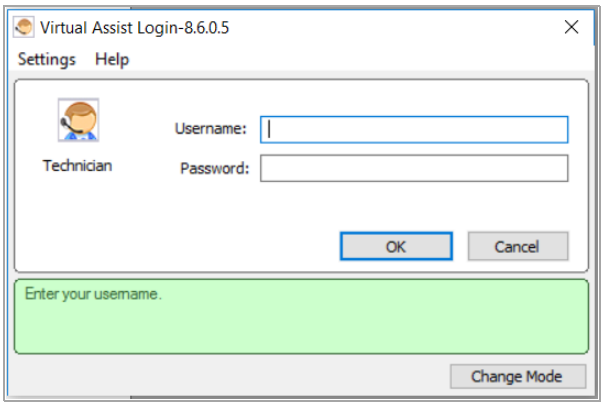
To launch a Virtual Assist Technician session to remotely assist customers:

1 Launch Virtual Assist and select the Technician Mode.



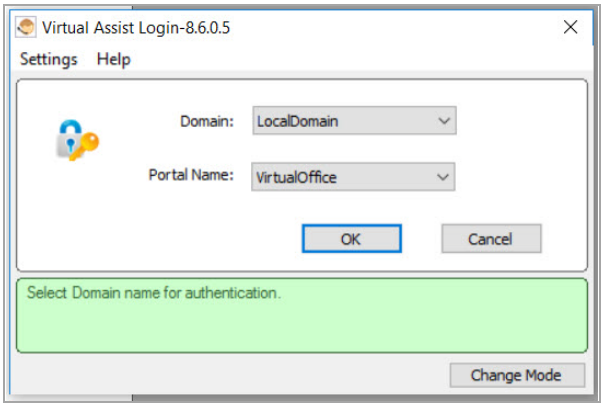
2 In the **Server** drop-down menu, select the IP address or domain name of the SMA/SRA appliance.

3 Click **Login**.



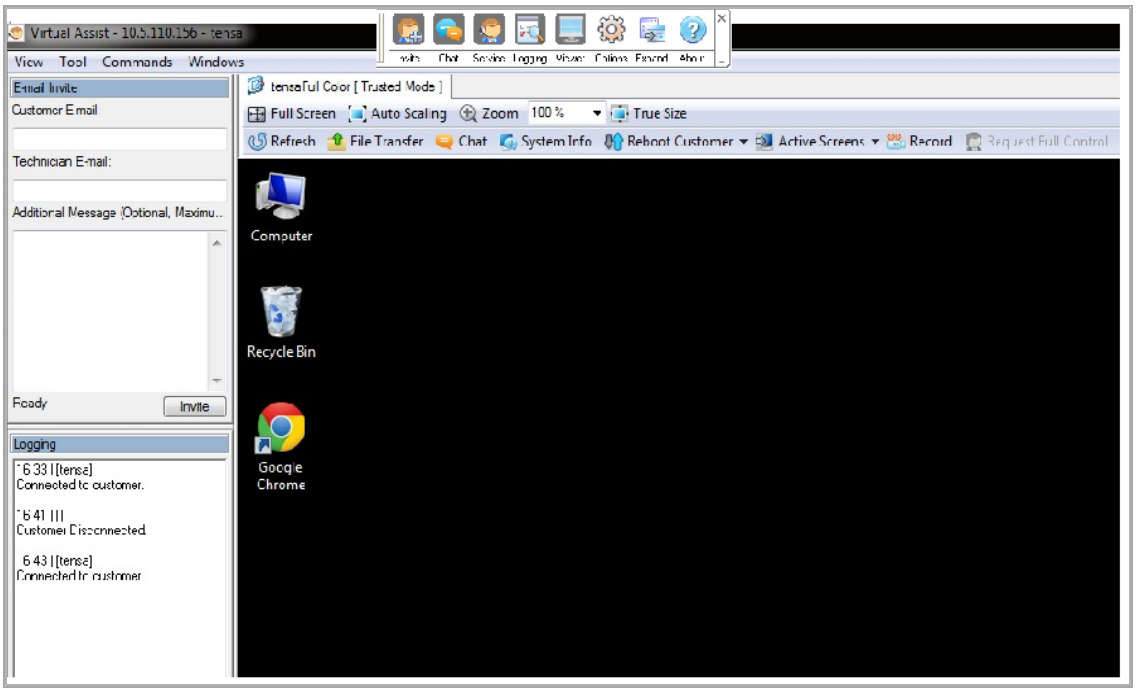
4 Enter the **Username** and **Password** for the Technician account on the appliance.

5 Click **OK**. The Select Domain window displays.



6 Select the **Domain** that the username is configured for and click **OK**.

7 The Secure Virtual Assist standalone application launches.



The Technician is now ready to assist customers.

Performing Secure Virtual Assist Technician Tasks

To get started, the Technician logs into the SMA/SRA appliance and launches the Secure Virtual Assist application.

NOTE: Each Technician can only assist one customer at a time.

By default, the Virtual Assist window launches with the Virtual Assist toolbar at the top and the rest of the window dedicated to the customer's screen. To display the most common panes, either click Expand or click **View > Classic Layout**. This displays the following panes:

- Email Invite
- Logging
- Chat
- Service

After the Technician has launched the Virtual Assist application, the Technician can assist customers by completing the following tasks:

- Inviting Customers by Email on page 71
- Assisting Customers on page 71
- Using the Windows Virtual Assist Taskbar and Tab Controls on page 72
- Using the Mac OS X Virtual Assist Taskbar and Tab Controls on page 74
- Using Additional Technician Commands on page 75
- Viewing Secure Virtual Assist Session Log on page 76
- Using the Secure Virtual Assist File Transfer on page 76

Inviting Customers by Email

To invite a customer to use Virtual Assist:

1 Using the email invitation form on the left of the Virtual Assist window, send the customer an invitation. If it is not displayed, click **Invite** in the toolbar.

> **NOTE:** Customers who launch Virtual Assist from an email invitation can only be assisted by the Technician who sent the invitation. Customers who manually launch Virtual Assist can be assisted by any Technician.

2 Enter the customer's email address in the **Customer Email** field.

3 Optionally, enter **Technician Email** to use a different return email address than the default Technician email. Some mail servers require that an email address be entered, and that it be on a valid domain.

4 Optionally, enter an **Additional Message** to the customer.

5 Click **Invite**. The customer receives an email with an HTML link to launch Virtual Assist.

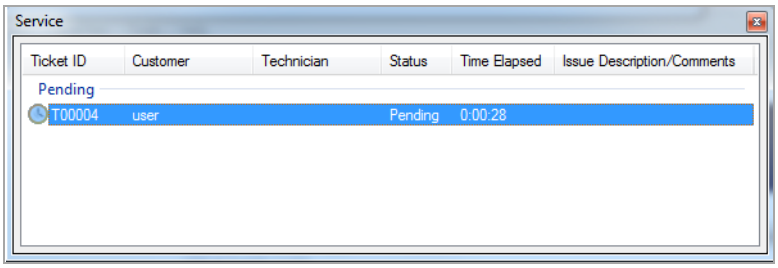
Customers requesting assistance appears in the Assistance Queue, and the duration of time they have been waiting is displayed.

Assisting Customers

A pop-up window in the bottom right task bar alerts the Technician when a customer is in the assistance queue. The customer queue is also displayed in the Service window.

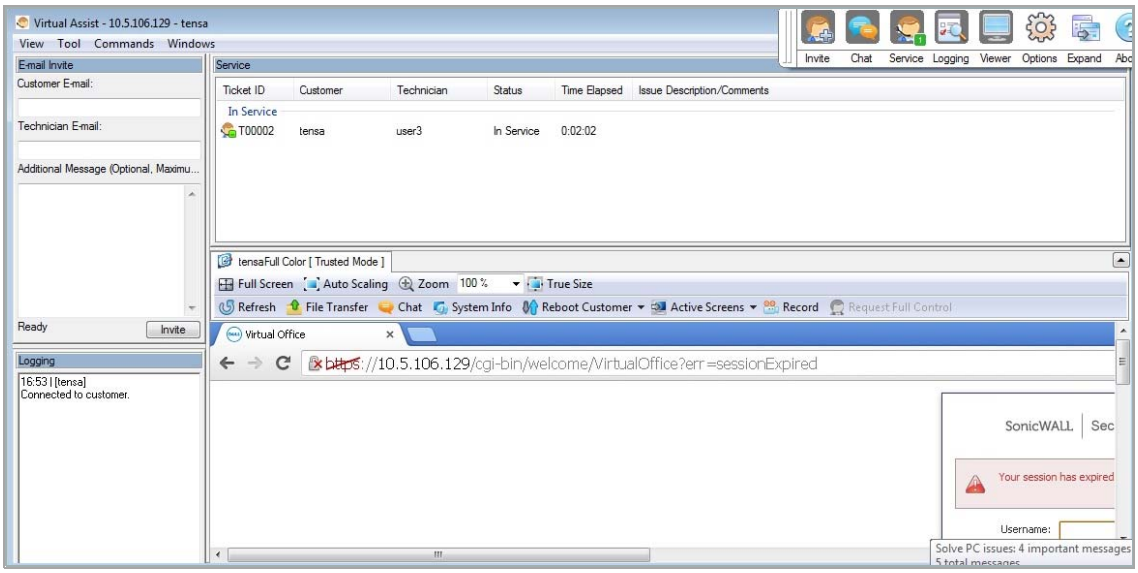
To assist a customer:

1 Double-click a customer's user name to begin assisting the customer.



> **NOTE:** Return a customer to the queue by right-clicking the user name on the Service List and selecting **Requeue**. Someone else in a Technician role can then service this user. This is useful if one Technician needs to hand off the user to another Technician, because of differing areas of expertise or the end of shift.

2 The customer's entire desktop is displayed in the bottom right window of the Secure Virtual Assist application.



The Technician now has complete control of the customer's keyboard and mouse. The customer can see all of the actions that the Technician does.

During a Virtual Assist session, the customer is not locked out of their computer. Both the Technician and customer can control the computer, although this might cause confusion and consternation if they both attempt "to drive" at the same time.

The small tool bar in the bottom right of the screen provides options during a Virtual Assist session:

- **Trusted/Active** - Toggles to the **View Only** mode, where the Technician can view the customer's computer but cannot control the computer.
- **Chat** - Initiates a chat window with the Technician.
- **End Virtual Assist** - Terminates the session.

Using the Windows Virtual Assist Taskbar and Tab Controls

The Technician's view of Virtual Assist includes a Taskbar with a number of options.

- **Invite** - Displays the Email Invite pane.
- **Chat** - Displays the chat window to communicate with the customer.
- **Service** - Displays the service queue of customers awaiting service.
- **Logging** - Displays the log window.
- **Viewer** - Displays or hides the entire Virtual Assist window.
- **Options** - Displays Connection Profile and Connection Settings options.
- **Expand** - Displays the Email Invite, Service, Logging, and Chat panes.

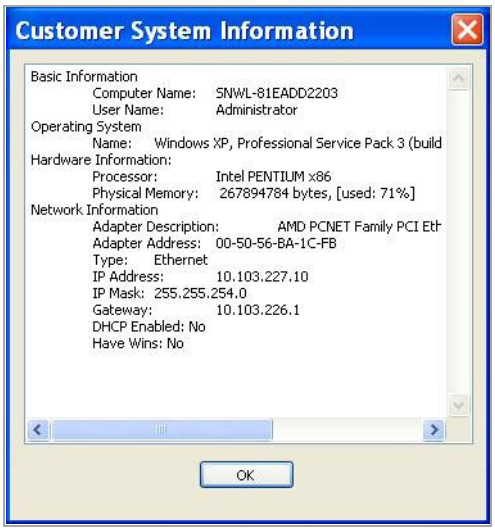
- **About** - Displays the version information for the Secure Virtual Assist client.

NOTE: Clicking the _ button in the bottom right corner of the Taskbar minimizes the view so only the titles of the buttons are displayed, and not the icons. Clicking **x** in the top right of the corner closes Virtual Assist.

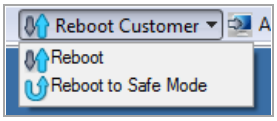
You can also display additional shortcuts and controls by selecting View > Tab Controls for Current Customer.

The following options appear at the top of the Virtual Assist window:

- **Full Screen** - Expands the Virtual Assist window to the Technicians entire monitor.
- **Auto Scaling** - Fits the customer's screen to the Virtual Assist window.
- **Zoom** - Customizes the zoom of the customer's screen.
- **True Size** - Zooms to the actual size of the customer's monitor resolution.
- **Gray Scale** - Change the display to gray scale instead of full color.
- **Refresh** - Refreshes the customer's screen.
- **File Transfer** - Opens the File Transfer utility. See Using the Secure Virtual Assist File Transfer on page 76 for more information.
- **Chat** - Opens a chat window with the customer.
- **Record** - Records the Virtual Assist session in a **.wmv** file that can be shared with other customers. The file is automatically named with the user name and the date and time the recording was started (for example, Sue_EST_2013-2-12_09h47m43s.wmv). The file location can be set on the Connection Settings window.
- **System Info** - Provides detailed information to the Technician about the customer's computer.

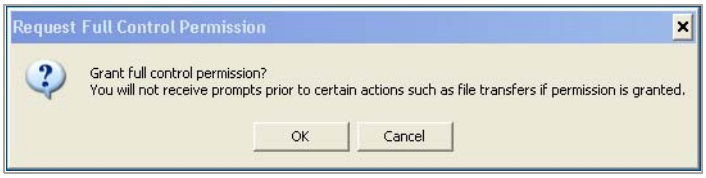


- **Reboot Customer** - Reboot the customer's computer. Unless you have Requested full control, the customer is warned about and given the opportunity to deny the reboot. You can select either a basic reboot or to reboot into Safe Mode with Networking.



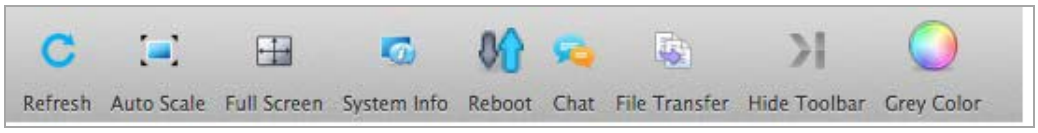
NOTE: When rebooting, you are prompted to enter the login credentials for the computer.

- **Active Screens** - Allows the Technician to switch to a second monitor if the customer's computer has more than one monitor configured, or display all monitors.
- **Request Full Control** - Technicians can request full control of a customer's desktop, allowing them to reboot the system, delete files, or over-write files on the customer's computer without the customer being repeatedly prompted for permission. Select Request Full Control under the Commands menu to issue a request that appears on the customer's desktop.



Using the Mac OS X Virtual Assist Taskbar and Tab Controls

In Mac OS X, the taskbar contains the following buttons:

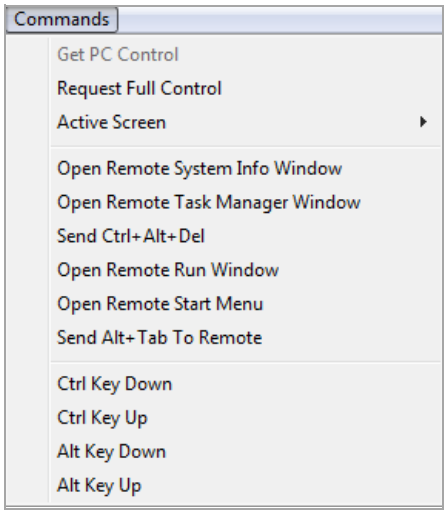


- **Refresh** - Refreshes the display of the customer's computer.
- **Auto Scale** - Adjusts the screen to fit the window size.
- **Full Screen** - Adjusts the screen to fill the entire window.
- **System Info** - Displays detailed information about the customer's computer similar to that shown for a Windows computer.
- **Reboot** - Reboot the customer's computer. Unless you have Requested full control, the customer is warned about and given the opportunity to deny the reboot.
- **Chat** - Launches the text chat window to communicate with the customer. The technician can also use the dedicated chat window in the bottom left window of the Secure Virtual Assist application.

- **File Transfer** - Launches a window to transfer files to and from the customer's computer. see Using the Secure Virtual Assist File Transfer on page 76 for more information.
- **Hide Toolbar** - Hides the taskbar from view.
- **Gray Color** - Displays everything in grey monochrome

Using Additional Technician Commands

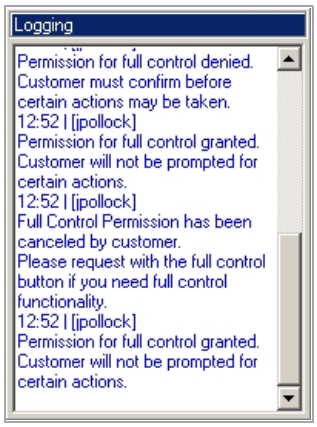
The Commands drop-down menu in the top left of the Virtual Assist window provides access to several of the options described above along with additional options.



- **Open Remote System Info Window** - Opens the System Info Window on the customer's computer.
- **Open Remote Task Manager Window** - Opens the Task Manager on the customer's computer.
- **Send Ctrl+Alt+Del** - Enters Control-Alt-Delete on the customer's computer.
- **Open Remote Run Menu** - Opens the Run menu on the customer's computer.
- **Open Remote Start Menu** - Opens the Start menu on the customer's computer.
- **Send Alt+Tab to Remote** - Enters Alt-Tab on the customer's computer to toggle between open windows.
- **Ctrl Key Down** - Engages the Control key on the customer's computer.
- **Ctrl Key Up** - Disengages the Control key on the customer's computer.
- **Alt Key Down** - Engages the Alt key on the customer's computer.
- **Alt Key Up** - Disengages the Alt key on the customer's computer.

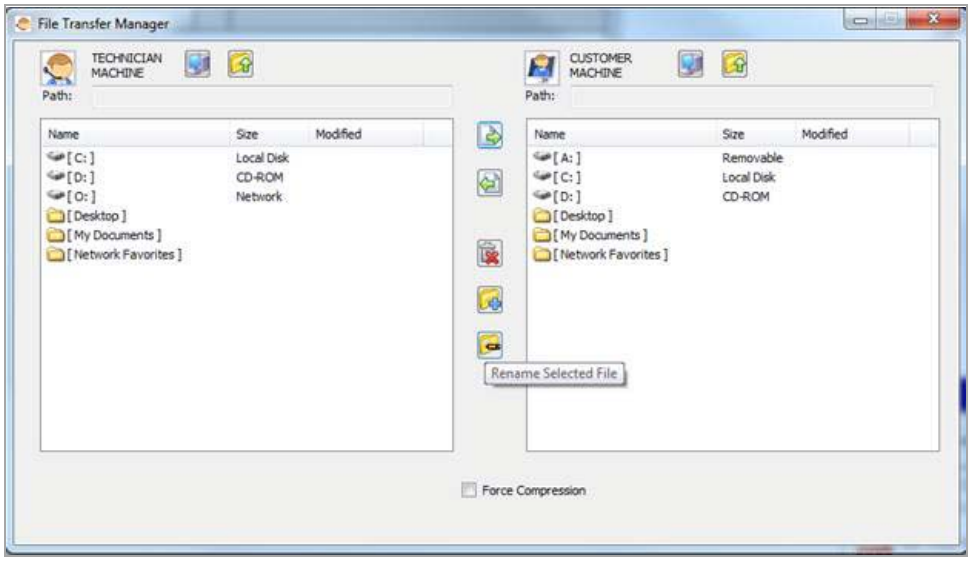
Viewing Secure Virtual Assist Session Log

The Secure Virtual Assist Session Log window can be displayed by clicking **Logging** in the Taskbar. The log displays a history of timestamped events for the session, such as opening Chat or File Transfer, requesting Full Control, and so on.



Using the Secure Virtual Assist File Transfer

The File Transfer window is used to transfer files to and from the customer's computer. The file directory of the Technician's computer is shown on the left and the customer's computer on the right.



The File Transfer window functions in much the same manner as Windows Explorer or an FTP program. Navigate the File Transfer window by double-clicking on folders and selecting files. The File Transfer window includes the following controls:

- **Desktop** jumps to the desktop of the Technician's or customer's computer.
- **Up** navigates up one directory on either the Technician's or customer's computer.
- **Download** transfers the selected file or files from the Technician's computer to the customer's computer.

- **Upload** transfers the selected file or files from the customer's computer to the Technician's computer.
- **Delete** deletes the selected file or files.

  NOTE: When deleting or overwriting files, the customer is warned and must give the Technician permission unless the Technician has clicked **Request Full Control** and the customer has confirmed.
- **New folder** creates a new folder in the selected directory.
- **Rename** renames the selected file or directory.

When a file is transferring, the transfer progress is displayed at the bottom of the File Transfer window. Click **Exit** to cancel a transfer in progress.

NOTE: File Transfer supports the transfer of single or multiple files. It does not currently support the transfer of directories. To select multiple files, hold down **Ctrl** while clicking on the files.

Initiating a Secure Virtual Assist Session from the Customer View

The following sections describe how to initiate and use Virtual Assist on the three supported client platforms:

- Initiating Secure Virtual Assist on a Windows Client on page 77
- Initiating Secure Virtual Assist on a Mac OS X Client on page 81
- Initiating Secure Virtual Assist on a Linux Client on page 84

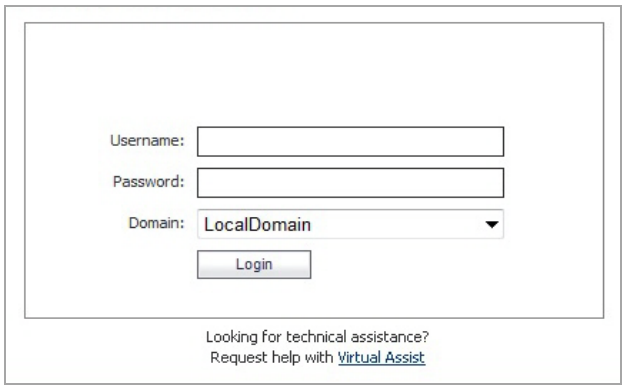
Initiating Secure Virtual Assist on a Windows Client

To launch a Virtual Assist customer session to request help on your Windows computer:

1 There are several methods for accessing Virtual Assist:

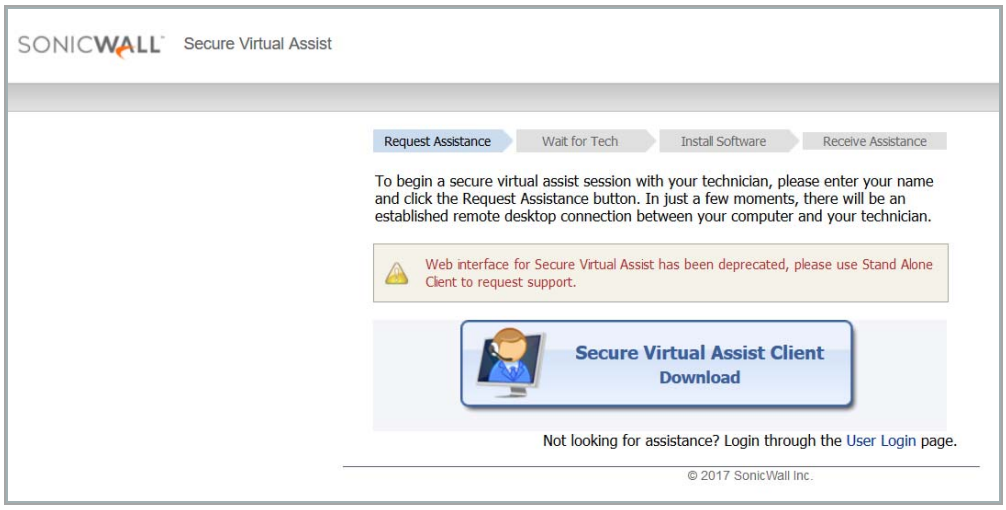
   - Navigate to the Virtual Assist home page using the URL provided by your Administrator or support Technician.
   - If you received an email invitation, click the link in the email or paste the URL into your Web browser.

- The login page of your Virtual Office can include a direct link to Virtual Assist as shown in the following paragraphs.



- Log in to the Virtual Office and click **Request Assistance**.

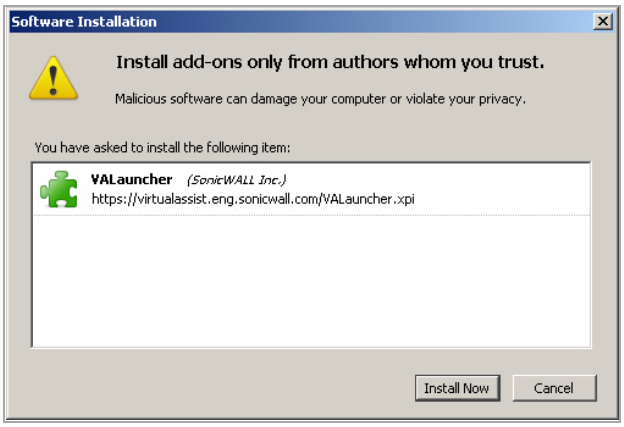
- If set by an administrator, click the **User Login** link. For Direct Interface, you can access three interfaces by accessing the URL: `supportLogin`, `vmLogin`, or `vmLoginCreator` link. The SMA Connect Agent replaces Active-X on these pages to launch the Virtual Assist and Virtual Meeting (on Windows and Macintosh) interfaces. There is a notification button bar on the pages for you to install the SMA Connect Agent. Click the active link and the following page appears:



- If Secure Virtual Assist has already been installed, select the Secure Virtual Assist shortcut from the Programs list under Window's **Start** button.

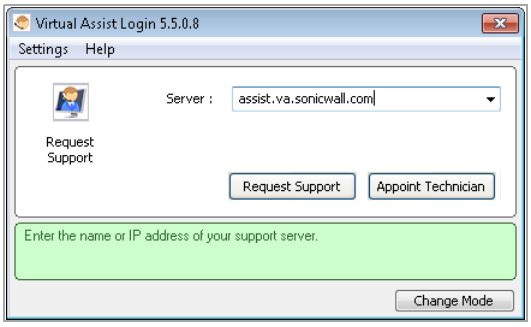
2 The first time you launch Secure Virtual Assist, you are prompted to install the Secure Virtual Assist plugin and client.

3 Click **Allow**. A plugin installation window displays. Click **Install Now**. The Secure Virtual Assist plugin and client installs. You might be prompted to restart your browser.



NOTE: Chrome browsers require installation of the plug-in from the Chrome store.

4 You can launch Virtual Assist either from the Virtual Office window or from a shortcut that is added to your Programs list under Window's **Start** button. If the **Server** address is not auto-propagated in the login window, enter the Server address. The server address can be either an IP address, IPv6 address, or hostname of the SMA/SRA appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).



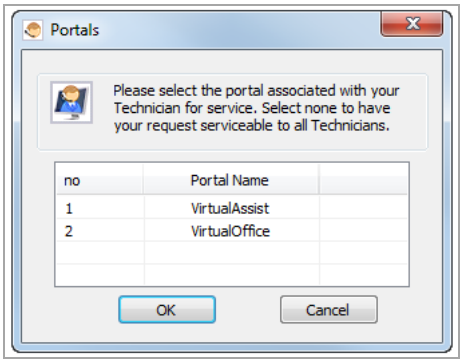
5 Click **Request Support** to request assistance or **Appoint Technician** to request assistance from a specific Technician.

6 If you receive the following security alert, click **Unblock** to allow Virtual Assist traffic through the Windows firewall.

7 If you selected **Appoint Technician**, a window listing all Technicians on duty appears. Select the Technician you would like to assist you and click **Request Support**.

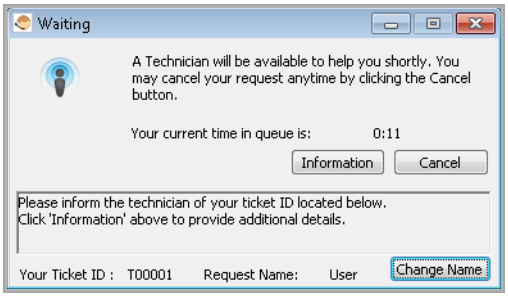
Your service request is displayed to all Technicians if you do not select a specific Technician. When you request a specific Technician, only that Technician sees your request.

8 Select the portal for the requested Technician and click **OK**. If you do not select a portal, you will be assisted by any Technician.



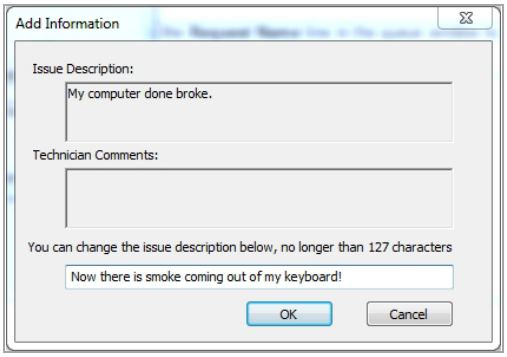
After selecting a portal, a certificate prompt appears, followed by an assistance code and/or disclaimer if configured by the Administrator.

9 A pop-up window indicates that you are in the Virtual Assist queue. The Technician is alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.

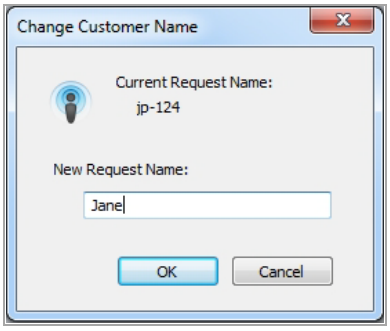


10 The Virtual Assist queue window provides two options:

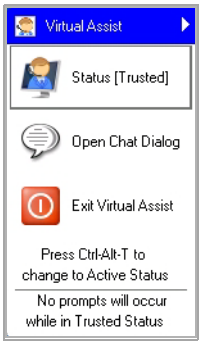
- Click the **information** to provide the Technician with information about your issue.



- Click the icon next to the **Change Name** line in the queue window to specify your name. By default, the computer name is used unless the customer responded to an email invite which displays the customer's email address.



11 When the Technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The Technician now has control of your computer.



12 For information on using Virtual Assist after the session is active, see Using Secure Virtual Assist on page 85.

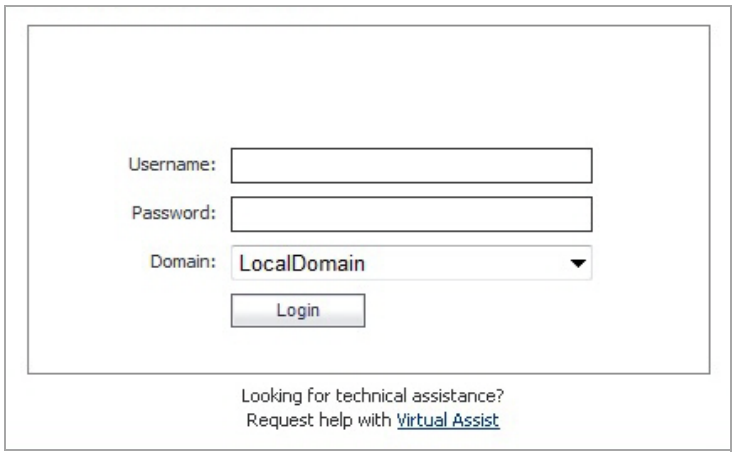
Initiating Secure Virtual Assist on a Mac OS X Client

To launch a Virtual Assist customer session to request help on your Mac OS X computer:

1 There are several methods for accessing Virtual Assist:

- Navigate to the URL of the Virtual Assist home page that is provided by your support Technician.
- If you received an email invitation, click the link in the email or paste the URL into your Web browser.

- The login page of your Virtual Office might include a direct link to Virtual Assist as shown in the following paragraphs.

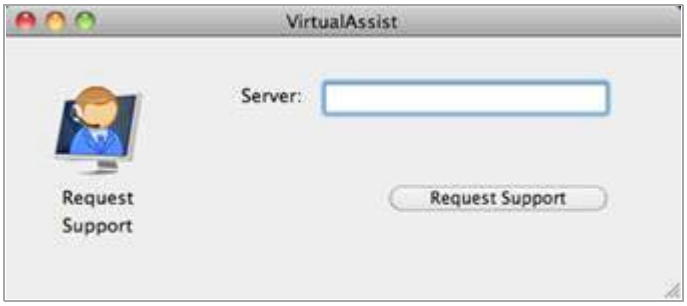


- Or you might need to log in to the Virtual Office and click **Request Assistance**.

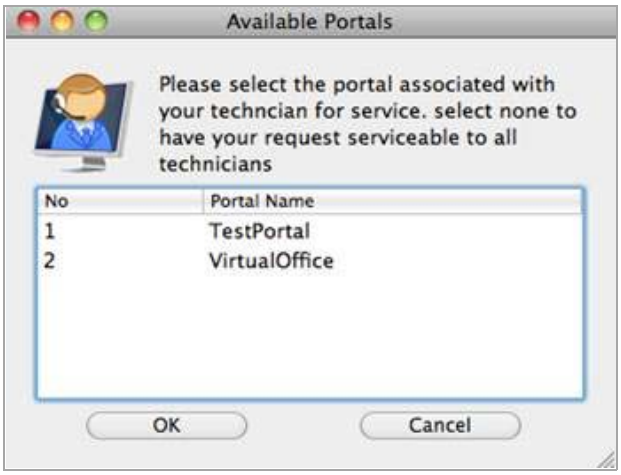
2 The first time you launch Virtual Assist, you are prompted to allow the Secure Virtual Assist applet to be installed on your computer. Click **Allow**.

3 The Secure Virtual Assist client installs and launches. In the future, you can either launch Virtual Assist either by navigating to the Virtual Office window in your browser, or you can launch it directly from your Applications folder.

4 If the **Server** address is not auto-propagated in the login window, enter the Server address and click **Request Support**. The server address can be either an IP address, IPv6 address, or hostname of the SMA/SRA appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).



5 The list of Available Portals is displayed. To connect to a specific portal, select it and click **OK**. To have your request be serviceable by all of the portals, click **OK** without selecting a specific portal.

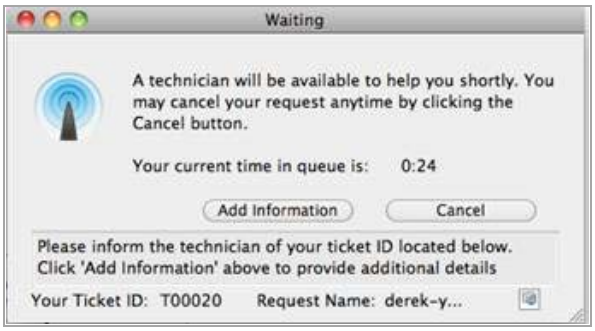


Your service request is displayed to all Technicians if you do not select a specific Technician. When you request a specific Technician, only that Technician sees your request.

6 You might be prompted to enter an **Assistance Code**.

7 If prompted to read and accept a disclaimer, click **OK**.

8 A pop-up window indicates that you are in the Virtual Assist queue. The Technician is alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.



9 The Virtual Assist queue window provides two options:

- Click **Add information** to provide the Technician with information about your issue.
- Click the icon next to the **Request Name** line in the queue window to specify your name. By default, the computer name is used.

10 When the Technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The Technician now has control of your computer.

11 For information on using Virtual Assist after the session is active, see Using Secure Virtual Assist on page 85.

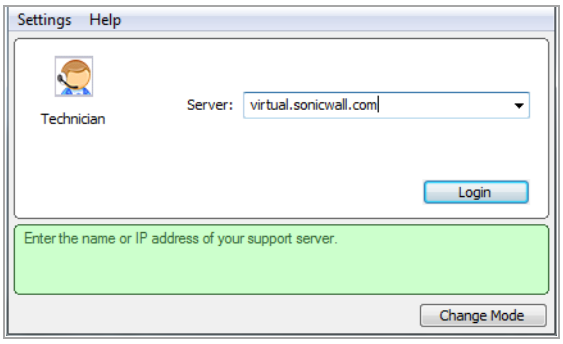
Initiating Secure Virtual Assist on a Linux Client

NOTE: SonicWall Secure Virtual Assist is fully tested on the Ubuntu distribution of Linux. It has not been tested on other Linux distributions.

To launch a Virtual Assist customer session to request help on your Linux computer:

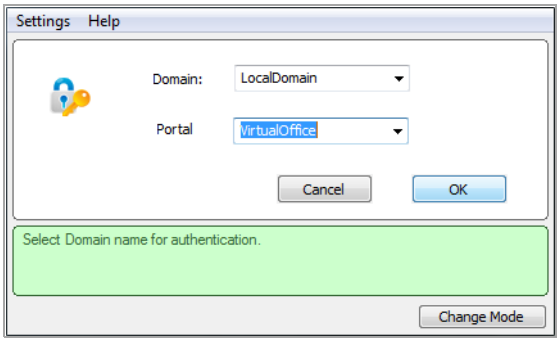
1 Launch Virtual Assist in the Technician Mode.

2 In the **Server** drop-down menu, select the IP address or domain name of the SMA/SRA appliance. Click **Login**.

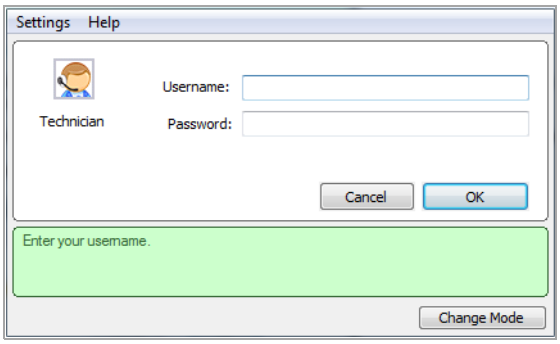


3 In the **Domain** drop-down menu, select the domain.

4 In the **Portal** drop-down menu, select the Virtual Office and click **OK**.



5 Enter the **Username** and **Password** for the Technician account on the appliance. Click **OK**. The Secure Virtual Assist standalone application launches.



Using Secure Virtual Assist

During a Virtual Assist session, you are not completely locked out of your computer. Both the Technician and customer can control the computer, although this might cause confusion and consternation if they both attempt to “drive” at the same time. You can resume control when the Technician is not actively typing or moving the mouse. And you can end the session at any time by clicking **End Virtual Assist** in the bottom right corner.

- Chatting with the Technician on page 86
- Changing the Secure Virtual Assist Level of Control on page 86
- Ending a Virtual Assist Session on page 86

Chatting with the Technician

To start chatting with the Technician assisting you, click **Chat** or enter **Alt-c** that opens an instant message chat session with the Technician. The Technician can also open a Chat window to communicate with you.

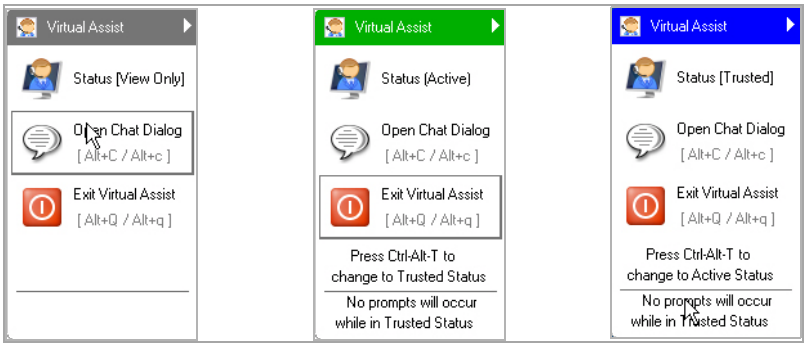
To chat with the Technician:

1. Click **Chat**.
2. Type text in the Chat window.
3. Press **Enter** or click **Send**.

Changing the Secure Virtual Assist Level of Control

There are three levels of control that a customer can grant to the Technician:

- **View Only** - The Technician can view the customer's computer but cannot control it. To switch to View Only mode, click **Status (Active)**. The Status switches to (View Only).
- **Active** - The Technician can control the customer's computer, but the customer must give permission for certain action—such as allowing the Technician to reboot the system, delete files, or over-write files on the customer's computer without the customer being repeatedly prompted for permission. To switch from View Only mode to Active mode, click **Status (View Only)**.
- **Trusted** - The Technician has complete control of the customer's computer. To toggle between Trusted mode and Active mode, enter Ctrl-Alt-T.



NOTE: By default, Virtual Assist sessions are launched in Trusted mode.

To modify the mode to a different level of control:

1. Click **Settings** on the top left corner of the window.
2. Select the **Connection Settings** tab.
3. Select either **Auto View Only** or **Active Mode**.

Ending a Virtual Assist Session

You can end the Virtual Assist session at anytime by clicking on **Exit Virtual Assist** in the bottom right corner of the screen, or by entering **Alt-q**. This ends the Technician's control of your computer.

Using Secure Virtual Assist in Unattended Mode

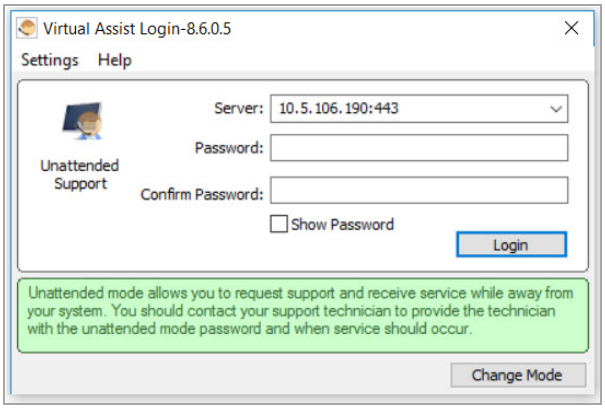
NOTE: Unattended Mode is supported only on Windows clients.

Unattended Mode allows customers to set their computer to be accessible by a Technician at a later time when the customer is not available to click to confirm their consent.

To configure Unattended Mode for Windows:

1 Launch Virtual Assist.

2 Click **Change Mode**, select **Unattended**, and click **Change Mode** again.



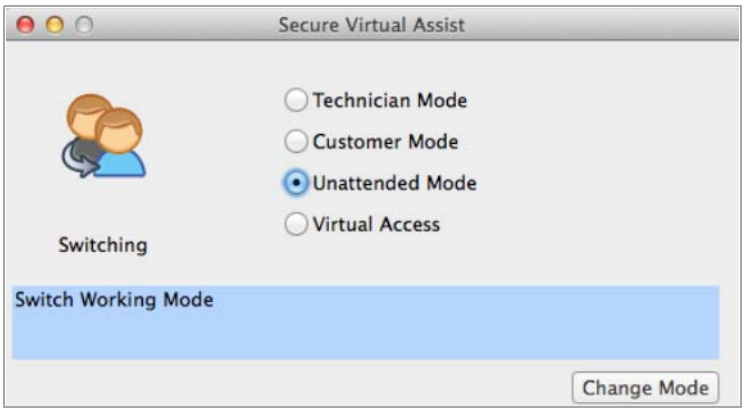
3 Select or enter the IP address or domain name of the SMA/SRA server.

4 Enter a **Password** and click **Login**. The Waiting window displays and shows the length of time you have been in the queue.

5 You need to provide the Technician with the password you just defined. An easy way to do this is to click **Add Information** and give the Technician your password.

To configure Unattended Mode for Mac OS X:

1 Select **Unattended Mode** on the Switch Working Mode window.



2 Click **Change Mode**. After the mode has changed, you are able to configure the Unattended Mode settings.

3 Specify the **Server** and **Password**. Then, log in to the server by clicking **Login**.

4 A wait screen displays until an available technician is available. Click **Appoint Technician** to select a technician. Click **Cancel** to cancel the request. Click Information to provide additional details.

NOTE: During Unattended Mode, the system must be kept active.

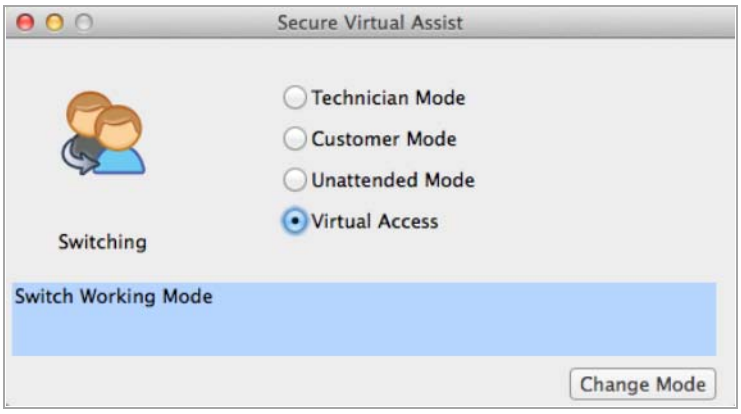
Using Virtual Access Mode

The Virtual Access feature allows Mac OS X users the availability to access their personal computers located out of LAN range from the SMA/SRA appliance.

NOTE: You must enable Virtual Access Mode from the **Portals** > **Portals** > **Virtual Assist Settings** page. Refer to the *SonicWall Secure Mobile Access Administration* documentation for more information.

To configure Virtual Access Mode:

1 Select **Virtual Access** on the Switch Working Mode window.



2 Click **Change Mode**. After the mode has changed, you are able to configure the Virtual Access settings.

3 Specify the **Server**, **Computer Name**, **Owner Name**, and **Password**. Then, log in to the server by clicking **Login**.

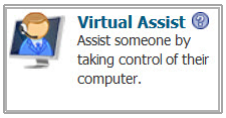
Enabling a System for Secure Virtual Access

Secure Virtual Access is similar to Secure Virtual Assist Unattended Mode in that Administrator privileges are required to install these client features, and a Technician is prompted to provide the password established during set-up to gain access to the system.

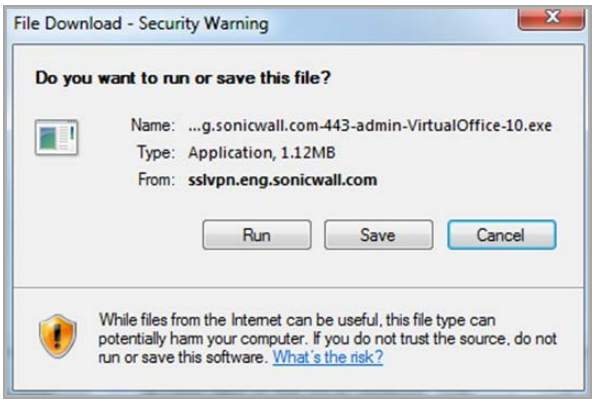
If Secure Virtual Access has been enabled on the Virtual Assist tab on the **Portals > Portals** page of the management interface, users see a link on the Virtual Office portal to set up a system for Secure Virtual Access.

To set up a system for Secure Virtual Access:

1 Log in to the Virtual Office portal through the system you wish to set up for Secure Virtual Access and click the **Virtual Access** link.



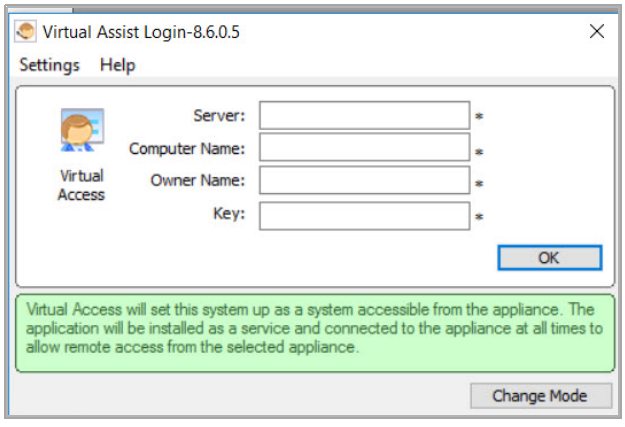
2 A file should download with parameters to install the VASAC.exe file that provides the needed client for Secure Virtual Access mode. Save and run the file.



NOTE: Running the file directly from this dialog box might not work on some systems. Save the file to the system and then run the application.

3 Fill in the necessary information in the provided fields to set-up the system in Secure Virtual Access mode and click **OK**.

- **Server:** This should be the name or IP address of the appliance the Technician normally accesses the Virtual Office from outside the management interface (Do not include “https://”).
- **Computer Name:** This is an identifier for the system to help differentiate between other systems that might be waiting for support in the queue. This name appears as a bookmark name in the user portal of the owner.
- **Owner Name:** This name must be a valid SMA/SRA appliance user name.
- **Key:** This is a key the Technician must enter prior to accessing the system through the support queue.



4 When prompted, enter the name of the Portal the Technician would normally log in to.

5 After installation, the VASAC client should be left running in the desktop tray.

This system's identifier name should now appear in the Technician's support queue displayed on the **Secure Virtual Assist > Status** page within the management interface.Upon double-clicking the system listing, the Technician is prompted to provide the password established during system setup to gain Secure Virtual Access to the system.

See also:

- Configuring Wake on LAN on page 90
- Ending Secure Virtual Access Mode on page 92

Configuring Wake on LAN

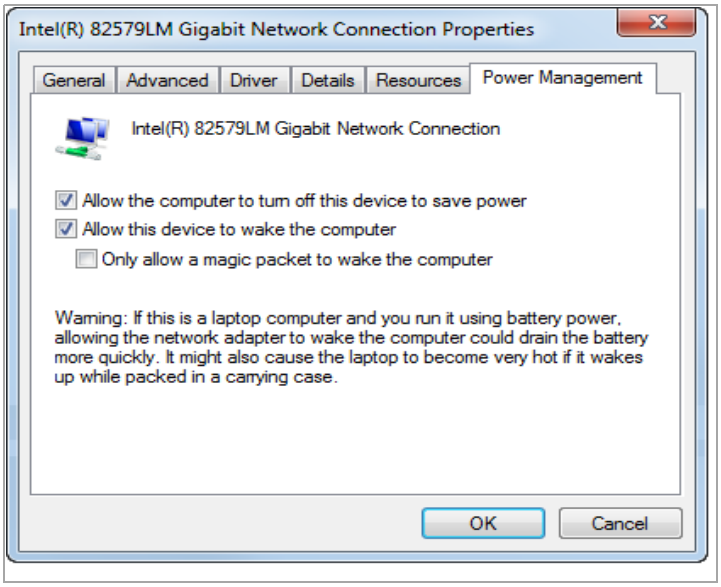
When operating in Secure Virtual Access mode, a customer can allow a Technician to wake a client running Virtual Assist on the LAN if both are in the same subnet. The client can be woken when powered off, in the Sleep state, or in the Hibernate state. This feature can be enabled globally, per portal, or from the client.

NOTE: To enable Wake Client, this feature must also be enabled on the portal and in the BIOS of the client machine.

To enable Wake on LAN on Windows:

1 Configure Wake on Lan in the client PC BIOS by selecting the **Wake-on-LAN** option.

2 Configure Wake on Lan in the client PC Device Manager:



a Open Device Manager by right-clicking the Computer icon on the client PC desktop, selecting **Properties** from the drop-down list, and then selecting Device Manager.

b Expand the Network adapters folder and select the Network Connection used for Virtual Access.

c Click the Power Management tab and select the **Allow the device to wake the computer** check box.

d Click **OK**.

3 While in the Secure Virtual Access mode, select **Enable WOL** from the Virtual Access menu.

If the client PC sleeps, shuts down, or hibernates, the pending client enters the Offline state, where it can be woken by a Technician.

4 Next, a Virtual Assist Technician double-clicks the customer's entry in the Pending List and the client PC is woken automatically.

NOTE: If the client PC cannot be woken, reinstall the Wake-on-Lan software, and reconfigure the client PC. The customer might end the service session at any time.

To configure Wake on LAN for Mac OS X:

1 Navigate to the **Portals** > **Portals** page on the SMA/SRA appliance, and click the **Configure** icon of the portal you want to enable Wake on LAN.

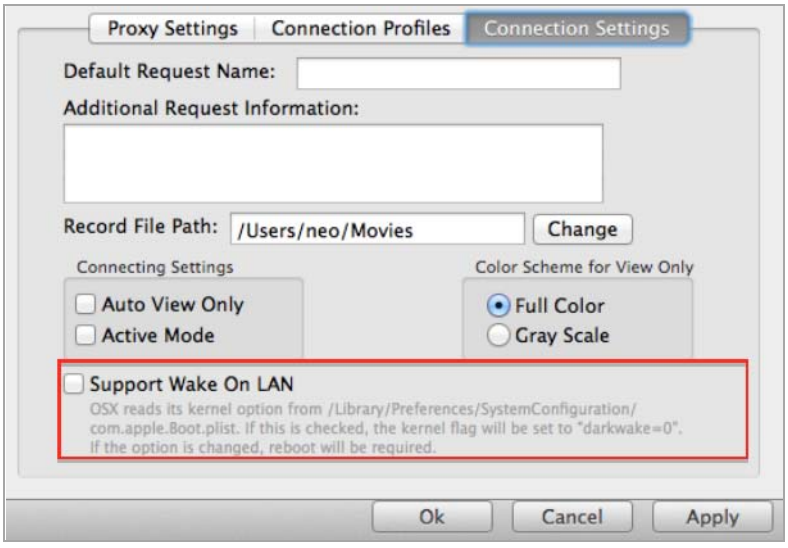
2 Click the **Virtual Assist** tab.

3 Select the **Enable Virtual Access Mode** check box.

NOTE: Virtual Assist must be enabled for the portal. Refer to the *SonicWall Secure Mobile Access Administration* documentation for more information.

4 Next, navigate to the Secure Mobile Access Virtual Assist Client Settings page.

5 Click on **Connection Settings**.



6 Select the **Support Wake on LAN** check box, and then click **OK**.

7 Select the Wake-on-LAN item from the Status pop up menu to enable the feature.

8 Navigate to **System Preferences > Energy Saver** to configure the system power settings.

9 Select the **Wake for network access** check box. Then, click **OK**.

Ending Secure Virtual Access Mode

Disconnecting from a Secure Virtual Access session places the system back in the support queue for later access by the Technician. From the personal system-side, the user/Technician might uninstall or terminate the application from the tray option icons.

An Administrator can forcibly remove a system from the queue. If this occurs, the Secure Virtual Access system should no longer attempt to connect to the support queue and should display an error message.

Using the Request Assistance Feature

If the **Display Request Help** option has been enabled on the Virtual Assist tab on the **Portals > Portals** page of the management interface, users see **Request Assistance** on the Virtual Office portal. By clicking this button on the portal, the user is placed in the Virtual Assist support queue for assistance.

For information on using Virtual Assist from the customer perspective, see Initiating a Secure Virtual Assist Session from the Customer View on page 77.

Using Secure Virtual Meeting

To set up a Virtual Meeting, the meeting Coordinator completes the following steps:

- Log in
- Schedule a meeting
- Invite meeting attendees

- Optionally, create a poll for the invited attendees
- Start the meeting
- Use meeting features during a meeting
- End the meeting

The functions you are allowed to complete depend on your role and whether a meeting is in progress. The following sections describe roles and how to use Secure Virtual Meeting:

- Overview of Roles on page 93
- Coordinator Role on page 94
- Participant Role on page 114

Overview of Roles

Secure Virtual Meeting has several user roles:

- **Coordinator** (Owner of the meeting) - The Coordinator must be a SMA/SRA user on the appliance. The Coordinator schedules, sets up, and controls the meeting. In addition, the Coordinator has the sole power to promote a Participant to the Assistant.
- **Assistant** (Coordinator-designated Assistant) - The Coordinator selects an Assistant from the list of available Participants and assigns the Assistant privileges. When the Coordinator exits the meeting, the Assistant automatically becomes the Coordinator. A meeting might have multiple Assistants, each with the same or a different set of privileges. An Assistant need not be a user of the SMA/SRA appliance. Possible Assistant privileges are:
    - Start/End Meeting
    - Set Host
    - Open Polling
    - Share Files
    - Set/Unset View Only
    - Invite Participants
    - Kick out Participants
    - Reschedule Meeting
- **Host** - The Host is a Participant who shares their desktop with all Participants in the meeting. When a meeting begins, the Host's desktop is shown to all Participants.

  The Host can be changed by the Coordinator during the meeting by selecting any available Participant. If a Host is not explicitly set when the meeting starts, the Coordinator becomes the Host. Only one Participant is designated as the Host at any one time.

  Only the Host can control the Host System, unless the Host grants permission when a Participant requests control. The Host might also give control to any Participant by selecting the Participant from the Meeting Members list. Only one Participant can control the Host System at any one time. When a Participant takes control of the Host System, he loses control as soon as the Host moves his mouse pointer on the screen. The meeting control permission state is visible to all Participants while in the lobby.
- **Participant** (User with credentials to join the meeting) - A Participant must enter a meeting code before they can join a meeting. The code required to join the meeting is determined by the Coordinator prior to the meeting. After joining a meeting, the Participant can view the shared desktop and chat with another

attendee privately or type a message in the Chat window that is visible to all attendees. A Participant becomes the Assistant if selected by the Coordinator or by an Assistant who has the required privilege.

- **View-only Participant** (User with limited meeting capabilities) - The Coordinator might designate any Participant as a View-only Participant. A View-only Participant cannot be assigned any privileges nor become an Assistant or Host.

Roles are switched before or during a meeting. A Coordinator or Assistant with necessary privileges can change the roles of any Participant during the meeting. A Participant wishing to become the Host must request permission from the Coordinator.

Coordinator Role

The Virtual Meeting Coordinator completes the tasks described in this section.

Coordinator tasks

Coordinator tasks	Description
Log In	Log in from a Virtual Meeting client using Secure Mobile Access credentials.
Set Up a Meeting	Set up a meeting by scheduling a time and creating a meeting code that allows meeting members to join the meeting.
Perform Lobby Functions	Access various meeting functions in the lobby before or during a meeting.
Control Roles	Control what meeting members can do and appoint an Assistant to help facilitate the meeting.
Revise Meeting Settings	Set up a proxy or modify login profiles for meetings.
Log Actions and Messages	Review a log of actions that occurred and view any warning or error message details that might require attention.
Start a Meeting	Start a meeting immediately or at the scheduled time.
Use the Control Menu During a Meeting	Access functions available while a meeting is active.
Create Email Invites	Invite meeting members through email before or during a meeting.
Poll Participants	Create a poll for attendees to participate in.
Use a White Board	Display a white board where objects, text, and highlighting can be added and view by Participants.
Share Files	Share a file with Participants that they can download.
Share Desktop	Share specific windows or all of your desktop with Participants.
Start Voice Conversations	Start a conversation where Participants can hear you.
Text Chat	Chat with everyone or specific individuals in a meeting.
Record meetings	Record meeting sessions in a .wmv file.

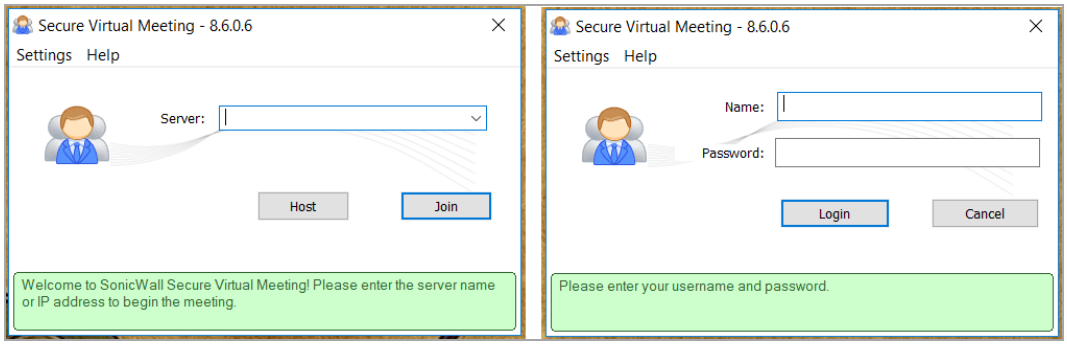
Topics:

- Logging In on page 95
- Setting up a Meeting on page 96
- Performing Lobby Functions on page 98
- Controlling Roles on page 99
- Revising Meeting Settings on page 101
- Logging Actions and Messages on page 102

- Using the Control Menu during a Meeting on page 103
- Creating Email Invites on page 105
- Polling on page 106
- Using a White Board on page 107
- File Sharing on page 108
- Sharing a Single Window on page 111
- Starting Voice Conversation on page 111
- Text Chatting on page 113
- Recording a Meeting on page 113

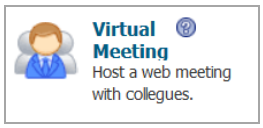
Logging In

A Participant can join a Virtual Meeting by clicking a link in the email invite or by logging into the Virtual Meeting client if the Administrator has enabled Join Without an Invitation on the AMC **Secure Virtual Meeting > Settings** page. To login from an installed Virtual Meeting, click **Host**.

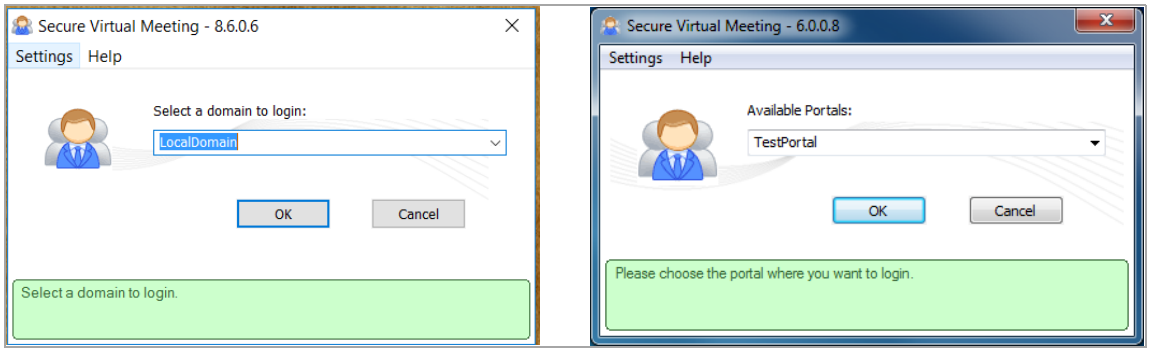


Only Secure Mobile Access users can be a Coordinator under normal circumstances, so Secure Mobile Access credentials are required for Coordinator login. However, a non-Secure Mobile Access user can become the Coordinator if the Participant is chosen as an Assistant and the Coordinator quits the meeting.

The meeting application can alternatively be accessed directly from the Virtual Office on an SMA 400, SRA 4600, and an SMA 500v Virtual Appliance.



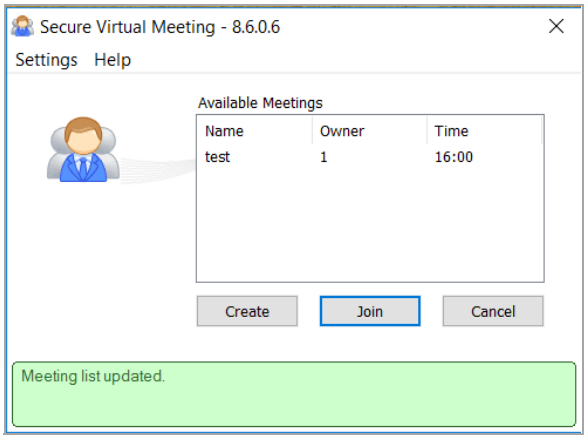
A **Domains** drop-down list is displayed if the user belongs to multiple domains, and a Portals drop-down list is shown if Virtual Meeting is enabled on multiple portals. Otherwise, the domain and portal is automatically selected.



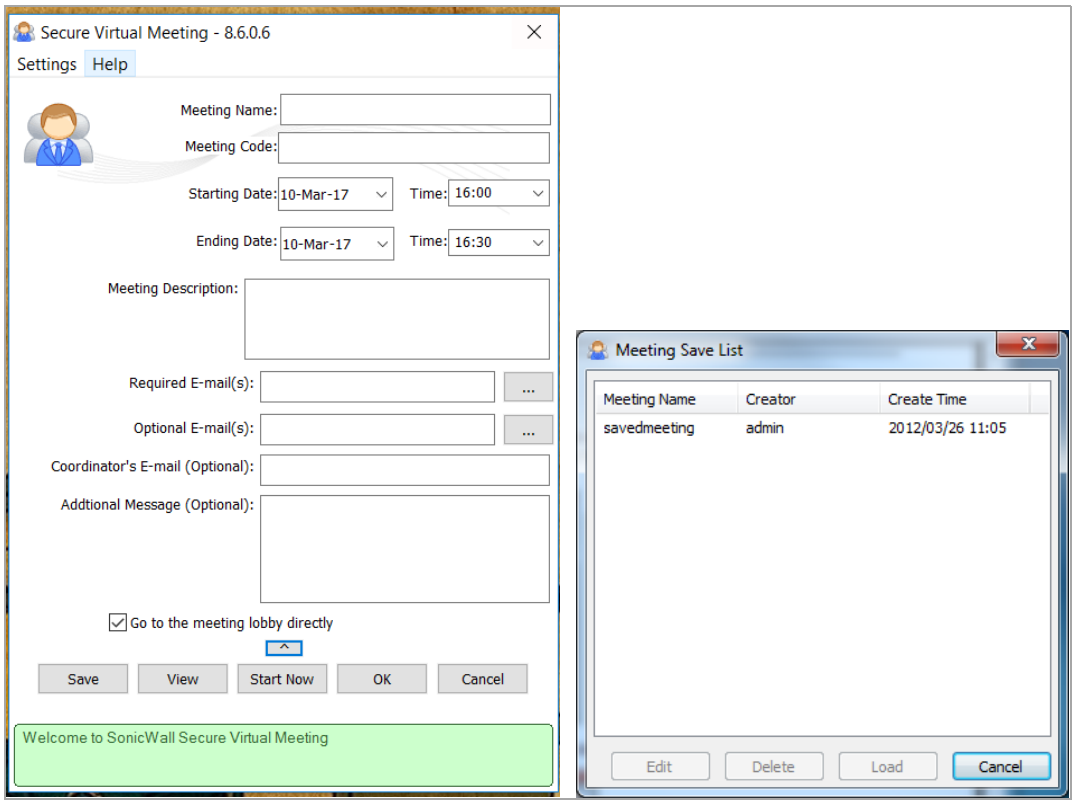
Select the desired portal to be used for the meeting. Only Participants who are in the selected portal are able to join the meeting.

Setting up a Meeting

After you are logged into the system, the option to create a meeting is available. If a meeting is already created you can view the details of the meeting by right-clicking the desired meeting and selecting **Properties**.



To create a meeting, click **Create** to display the meeting creation interface.



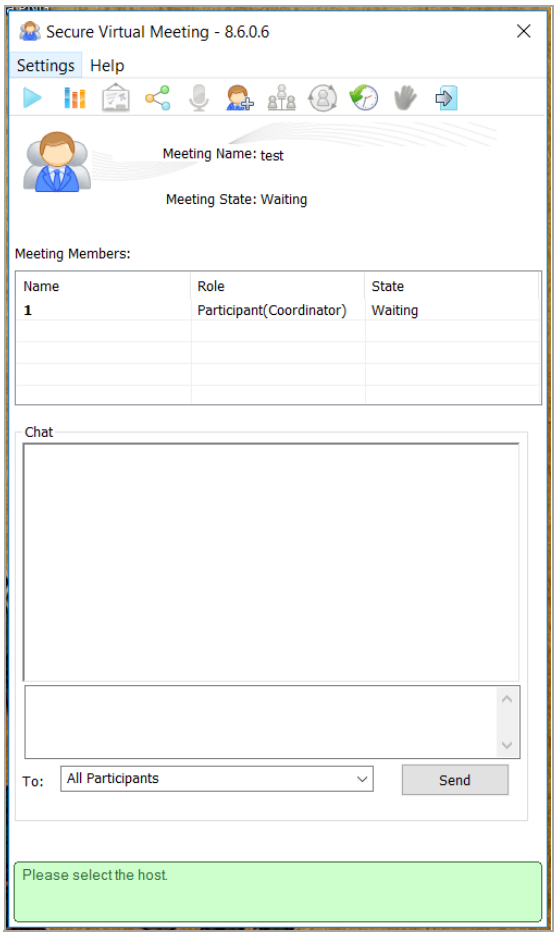
To set up a meeting enter a **Meeting Name, Meeting Code, Starting Date** and **Time**, and **Ending Date** and **Time**. The meeting code is entered by all Participants wishing to join the meeting. If you want to invite attendees and the Email fields are not visible, click the down arrow directly below the **Ending Date** field. You can then identify who should receive meeting email invitations.

Use the buttons across the bottom of the window to complete the following functions:

Settings window: Buttons

Save	Saves the meeting for future editing.
View	Displays previously saved meetings.
Start Now	Starts the meeting immediately with the current user system time, and enter the lobby.
OK	Start the meeting immediately at the next available time slot (based on the current time), and enter the lobby.

After you create a meeting, you enter the meeting's lobby automatically.



When a meeting is scheduled for a later time, the Coordinator exits the meeting and returns to the lobby at the meeting start time. If the **Allow starting meeting without meeting creator** setting is disabled and the Coordinator has not joined the meeting by the start time, the participants are kept waiting in the lobby until the scheduled meeting end time (when all participants automatically exit the lobby). If the **Allow starting meeting without meeting creator** setting is enabled and the Coordinator has not joined the meeting by the start time, within two minutes past the scheduled start time, an existing participant is chosen randomly to become the Coordinator.

If the Coordinator enters but does not start the meeting, when the meeting time ends the Coordinator receives a notification to reschedule or end the meeting. When the end time is reached, the meeting ends and all meeting members automatically exit the meeting.

In the lobby you can manage the meeting, set roles, and many other functions described in Performing Lobby Functions on page 98, depending on your role.

Performing Lobby Functions

The following functions can be completed from the lobby by clicking buttons at the top:

Clicking **Start Meeting** starts the meeting. Only the Coordinator and Assistant can start a meeting.

When a meeting is started, **Start Meeting** changes to **Stop Meeting**. Clicking **Stop Meeting** ends the meeting. Only the Coordinator and Assistant can end the meeting.

Clicking **Polling** opens the polling window where you can load, edit, and start a poll for Participants currently in the meeting. Only the Coordinator and Assistant can initiate polling. Polling details are described in Polling on page 106.

Clicking **White Board** displays a white board to all meeting Participants where the Coordinator can add objects, text, and highlighting. White board is available only during a meeting. White board details are described in Using a White Board on page 107.

Clicking **File Share** opens the file share window where you can select files for Participants to download and monitor Participants' downloads. Only the Coordinator and Assistant can initiate file sharing. Details are described in File Sharing on page 108.

Clicking **Start Voice Conversation** shares voice communication with Participants in the meeting lobby. Only the Host can be heard. Voice Conversation details are described in Starting Voice Conversation on page 111.

When a voice conversation is started, **Start Voice Conversation** changes to **Stop Voice Conversation**. Clicking **Stop Voice Conversation** ends voice communication.

Clicking **Invite** sends an email invitation to Participants. Only the Coordinator and Assistant can invite Participants. Invite details are described in Creating Email Invites on page 105.

Clicking **Start Sharing** shares the Host desktop with all Participants in the meeting. Sharing is only available during a meeting.

When a desktop is being shared, **Start Sharing** changes to **Stop Sharing**. Clicking **Stop Sharing** stops sharing the Host System desktop. Only the Host can stop sharing.

Clicking **Request Control** requests that the Host give you control of the keyboard and mouse. Only Participants who are not the Host can request control.

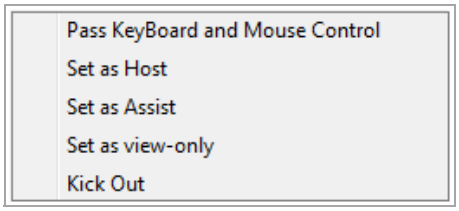
Clicking **Reschedule Meeting** reschedules the meeting start and end times. Only the Coordinator and Assistant can reschedule a meeting.

Clicking **Request Host** informs the Host that you want to become the Host and share your desktop. Only Participants who are not currently the Host can request to become the Host.

Clicking **Quit** exits the meeting and return to the meeting selection window. Anyone in the meeting can quit the meeting.

Controlling Roles

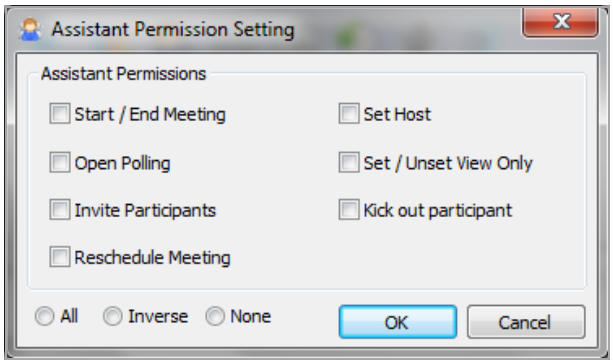
The Coordinator and Assistant can change a meeting member's role by right clicking the meeting member's name and selecting a role from the drop-down menu.



The following options could appear, depending on permissions and the meeting member's current role.

Options based on assigned role

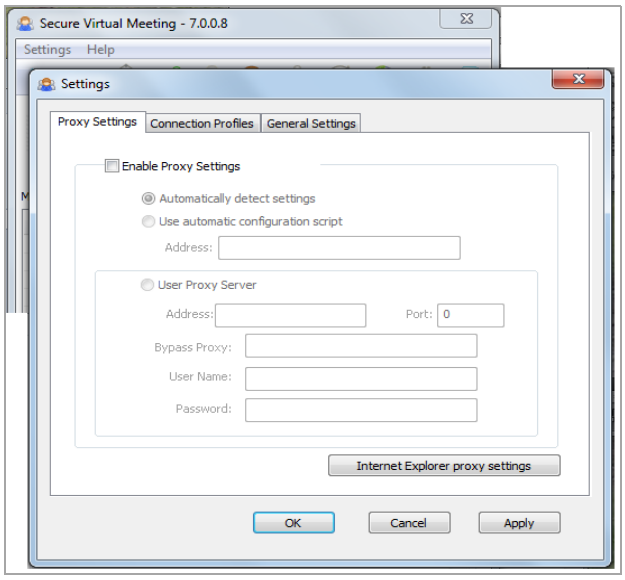
Option	User	Description
Pass Keyboard and Mouse Control	Host	Allow the selected Participant to control the Host's PC.
Set as Host	Coordinator Assistants with Set Host permission	Set the selected Participant to be the Host.
Set as Assistant	Coordinator	Set the selected Participant to be the Assistant. An Assistant has privileges similar to the Coordinator, depending on the settings selected by the Coordinator as shown below.
Set as view-only	Coordinator Assistant	Set the selected Participant to view-only mode so the Participant can only view the Host desktop (cannot request control).
Kick out	Coordinator Assistant	Remove the selected Participant from the meeting.



Revising Meeting Settings

Proxy Settings

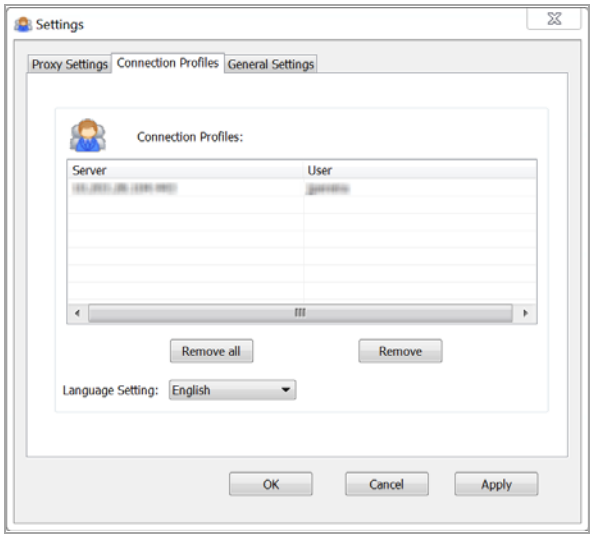
For setups requiring a proxy, click **Proxy Settings** in the Virtual Meeting window. Select **Enable Proxy Settings**.

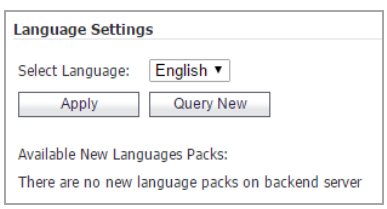


Enter the proper information to utilize the proxy or click the **Internet Explorer proxy settings** button to automatically import the proxy settings used by Internet Explorer.

Connection Profiles

For users accessing different appliances, profiles are shown on the Connection Profiles window. Information about the server currently in use is automatically populated for convenience.



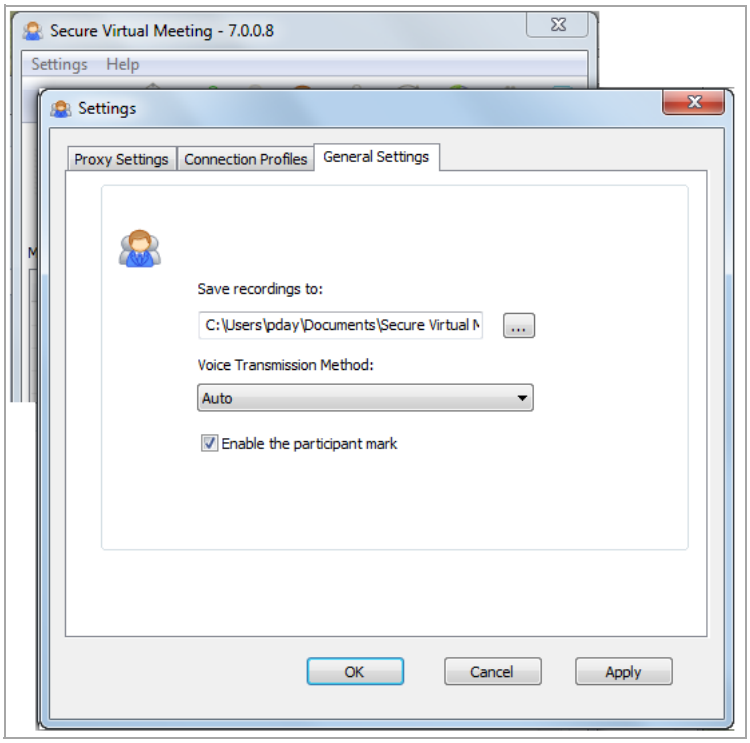


To remove all connection profiles, click **Remove All**. To remove a specific connection profile, select the connection profile and click **Remove**.

The Connection Profiles window also provides the ability to change the language settings. By default, the language is English. You can change the language by selecting one from the drop-down menu and clicking **Apply**. You can also search for additional language packs to download from the backend server by clicking **Query New** to find and import a .zip file language package. After the import is complete, the client adds the language pack and it is available from the drop-down menu.

General Settings

The General Settings tab is used to select the location where recordings are saved, select the Voice Transmission method, and enable or disable the Participant Mark feature.



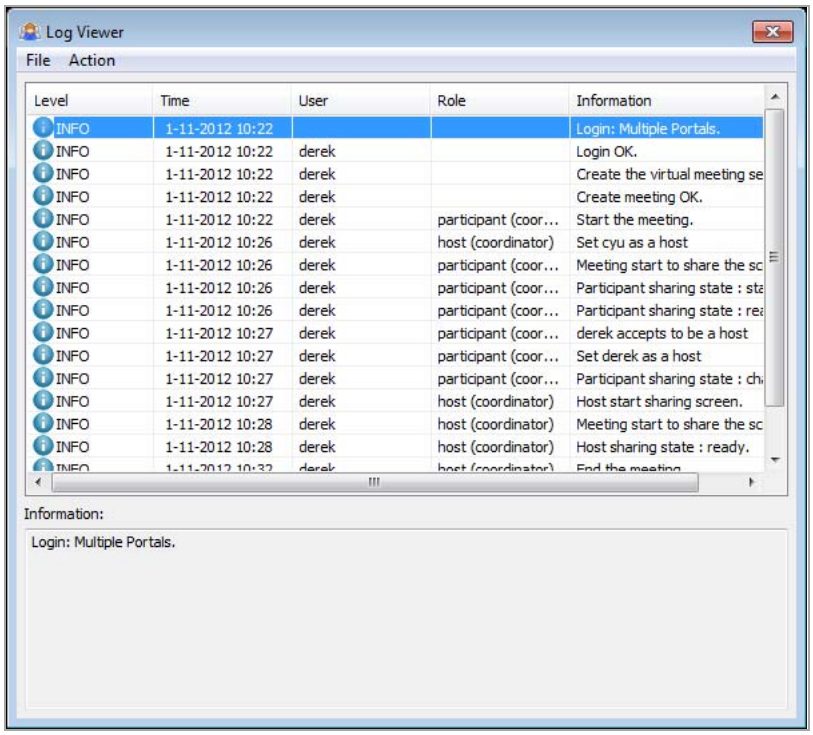
To change the default settings:

- Click ... **Browse** and select the location where you want to save meeting recordings.
- Select the protocol to use for transmitting voice conversations from the **Voice Transmission Method** drop-down list.
- Select the **Enable the participant mark** check box to enable this feature. The Participant Mark feature that is enabled by default, allows Participants to double-click something on the Host's desktop while it is being shared to call the Host's attention to it. The Participant Mark is displayed on the shared desktop in the area where the Participant double-clicked.

Logging Actions and Messages

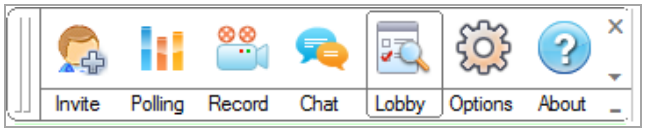
The Log Viewer displays all event log data that includes actions taken during a meeting and any errors that occur. The Log helps you keep track of events that occur in a meeting and shows all actions completed by

meeting Participants. Use the error and warning events in the log to take the appropriate corrective action, if necessary.



Using the Control Menu during a Meeting

The Control Menu is available at the top of a shared desktop when the Host shares the desktop during an active meeting.



The **Invite** button is available for the Coordinator or Assistants with invite permission. It opens the invite dialog if the lobby is not open. Invite details are described in Creating Email Invites on page 105.

The **Polling** button is available for the Coordinator or Assistants with polling permission. It opens the polling dialog detailed in Polling on page 106.

The **Chat** button is available for all Participants, including View-only Participants. It opens a chat dialog if the lobby is not open. Chat details are described in Text Chatting on page 113.

The **Lobby** button is available for all meeting members, including View-only Participants. If the lobby is hidden during a meeting, it displays the lobby window when the Host is sharing the screen.

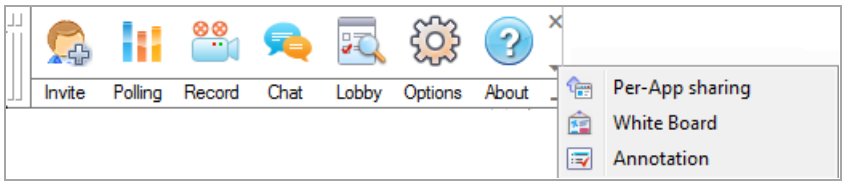
The **Options** button opens the Meeting Settings window described in Revising Meeting Settings on page 101 and is available for all Participants.

The **Viewer** button is available for all Participants except the Host. It toggles the window between the Participant's window and the Host's desktop.

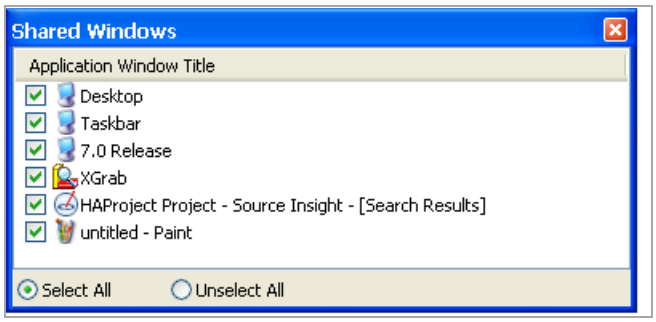
The **About** button opens the About dialog that identifies the Secure Virtual Meeting client and version. The **About** button is available for all meeting members, including View-only Participants.

In addition, Participants can double-click something on the Host's desktop while it is being shared to call the Host's attention to it. The Participant Mark is displayed on the shared desktop in the area where the Participant double-clicked. This feature that is enabled by default, is enabled/disabled on the **Settings > General Settings** tab.

The drop-down arrow shown on the right of the Control Menu opens a list of additional features: Per-App Sharing, White Board, and Annotation:



Per-App Sharing allows the Coordinator to select specific windows to share with meeting Participants instead of sharing the entire desktop. Selecting this feature displays a window where the windows are chosen.

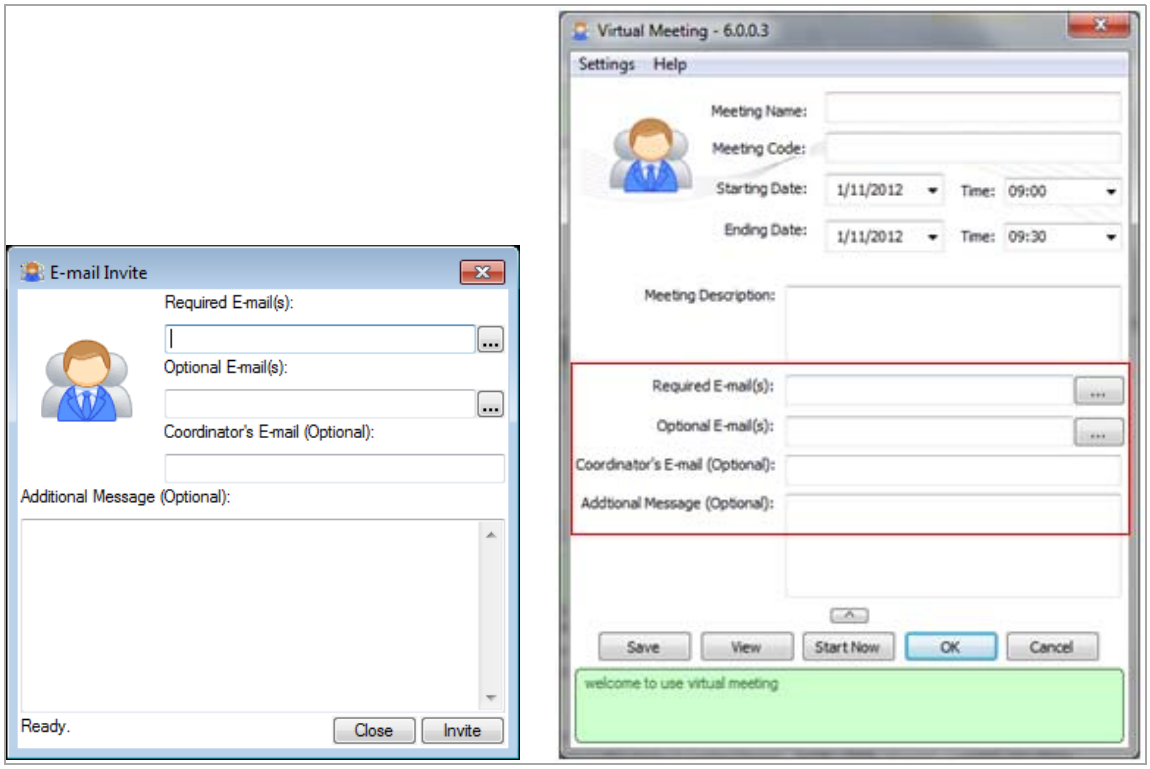


White Board displays a white board and is also displayed on the Lobby toolbar. See Using a White Board on page 107 for additional information.

Annotation allows any meeting Participant to add text, objects, and highlighting to a white board using the white board toolbar.

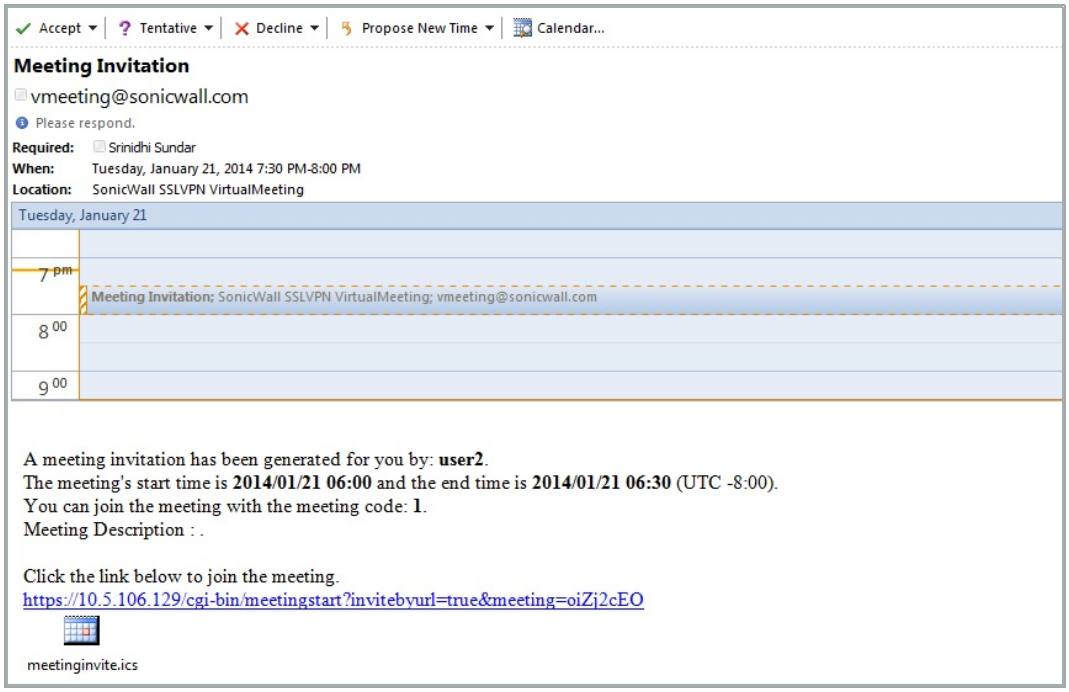
Creating Email Invites

Invitations can be sent when creating the meeting or while in an active meeting.



NOTE: Email settings must be configured in the management console **Log > Settings** page before Virtual Meeting email can be sent.

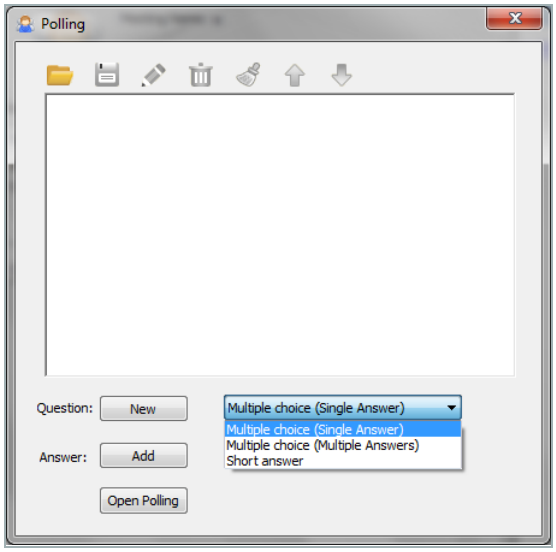
To invite someone to a Virtual Meeting, enter the email address and click **Invite**. Additional fields are optional. Invited users receive an email similar to the following:



After receiving the email invitation, attendees click the link in the email that accesses the appliance to join the meeting. If the Secure Virtual Meeting plug-in is installed, it automatically downloads and launches the application and puts the attendee into the meeting. Alternatively, attendees can manually download the Secure Virtual Meeting plug-in and run it as an application. Both cases provide meeting access.

Polling

Click Open Polling to display the Polling window where you can create polls and define the polling questions.



Create new questions by clicking the and buttons. There are three question types:

- Multiple choice (single answer)
- Multiple choice (multiple answer)
- Short answer

Use the buttons at the top of the window to:

The **Open Virtual Meeting Poll Files** button opens any saved polling questions and possible answers.

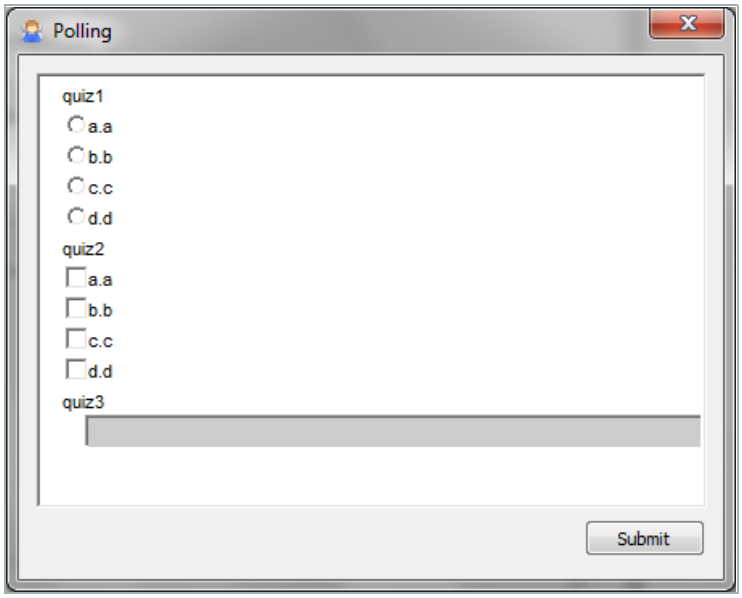
The **Save Virtual Meeting Poll File** button saves the current polling questions and answers.

The **Edit** button is used to edit the currently selected polling question or answer.

The **Clear** button erases ALL polling questions and answers.

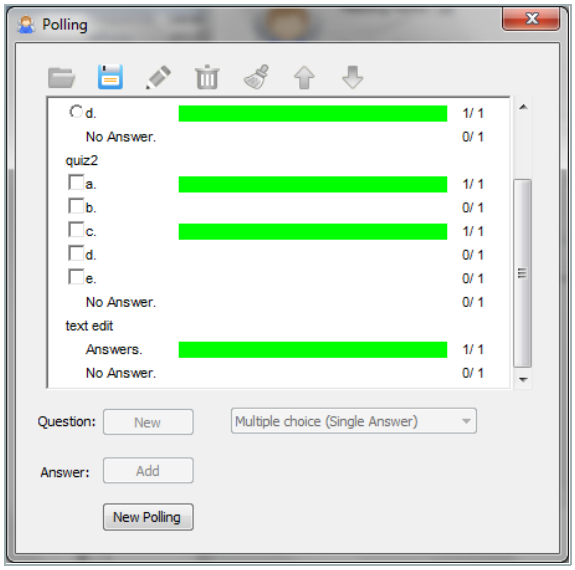
The **Up** and **Down** buttons change the order of the selected questions or possible answers.

Click Open Polling to start polling and send the poll to the selected Participants to answer.



Polling feedback window

Feedback from the poll is returned to the poll initiator when answers are submitted and when **End Polling** is clicked. The collected feedback is displayed as shown below. Click the green bar to display detailed information for each answer.



Using a White Board

The Host can share a white board with Participants. Text, objects, and highlighting that can be customized, are added to the white board using the toolbar at the top of the white board.

The white board contains the following tools:

Select tool is a pointer used to point to objects on the white board. The user cannot add anything on the white board until another tool is selected.

Pen tool is used to draw a freehand shape. The pen's color (default black) and line width (1-100pt, default 8pt) are configurable with the Customization tools.

Highlighter tool is another kind of pen used to draw a transparent freehand shape. The highlighter width (1-100pt, default 16pt) and transparency saturation (1-100, default 50) is configurable with the Customization tools. The transparency saturation is adjusted by

Line tool draws a straight line. The line color (default black) and weight (1-100pt, default 10pt) are configurable with the Customization tools.

Rectangle tool draws a rectangle. The rectangle edge color (default black), fill color (default transparent), and edge weight (1-100pt, default 5pt) are configurable with the Customization tools.

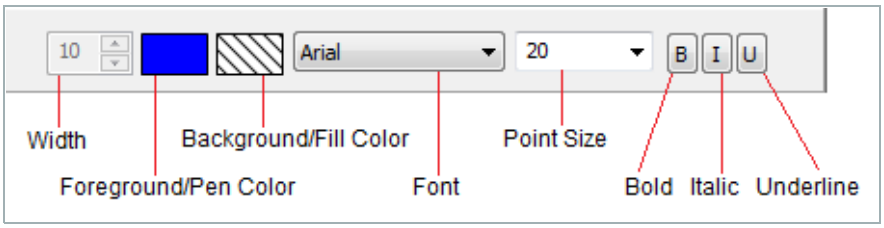
Ellipse tool draws an ellipse on the white board. The ellipse color (default black), fill color (default transparent), and edge weight (1-100pt, default 5pt) are configurable with the Customization tools.

Text tool adds text on the white board. The text's color, font, font size, and style (default Arial 20pt) are configurable with the Customization tools.

Eraser tool erases anything on the white board. The eraser width (default 20pt) is configurable with the Customization tools.

Clear All Contents tool erases all contents on the white board.

Customization Tools:



File Sharing

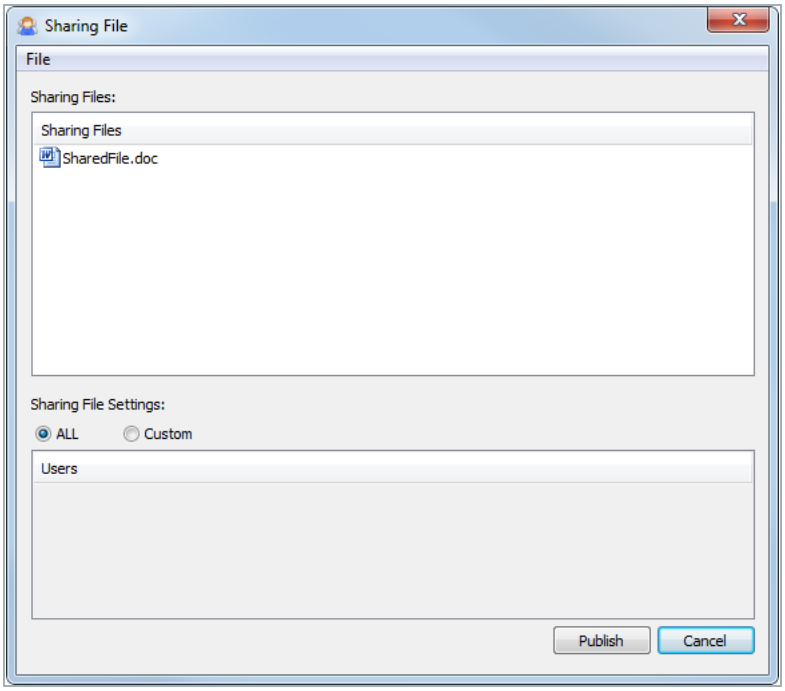
The Host can share files with Participants during a meeting. See the following:

- Sharing Files on Windows on page 109
- Sharing Files on Mac OS X on page 110

Sharing Files on Windows

To share files with participants on Windows:

1 Click File Sharing to display the File Sharing window where you can select a file to share with Participants and monitor downloads.



2 To share a file, select **File > Select File** from the menu on the Sharing File window and select the file.

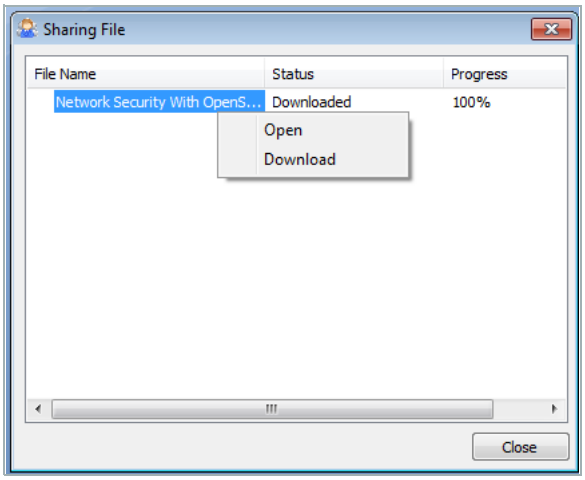
3 By default, the file is shared with all meeting Participants. To share the file with specific meeting Participants select **Customize**.

4 Next, click **Publish** to notify Participants that a file is available for download.

To change the list of Participants who can download the file, right-click the file and select **Setting** at any time. To remove the file from the download list, right-click the file and select **Remove** at any time.

5 When a file is published, the selected Participants receive a notification in the lower right corner of their screens.

6 Download the file by clicking **File Sharing**, right-clicking the file and selecting **Download**, and then right-clicking the file and selecting **Open** after the file has downloaded.



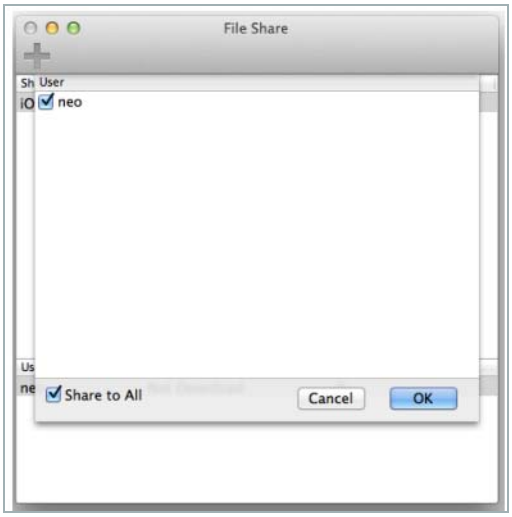
Sharing Files on Mac OS X

To share files with participants on Mac OS X:

1 Click **File Sharing** to display the File Sharing window where you can select a file to share with Participants and monitor downloads.

2 To share a file, click **Add** from the menu on the Sharing File window and select the file.

3 To share the file with all meeting Participants, select **Share to All**. To share the file with specific meeting Participants, select the Participants. Then, click **OK**.



4 The list of Participants displays on the lower section of the File Share window. The files shared are listed at the top section of the File Share window.

To remove a file from being shared, right-click the file in the window and select **Remove**.

To reset the file share download list, right-click the file in the window and select **Setting**. The Setting window displays additional options.

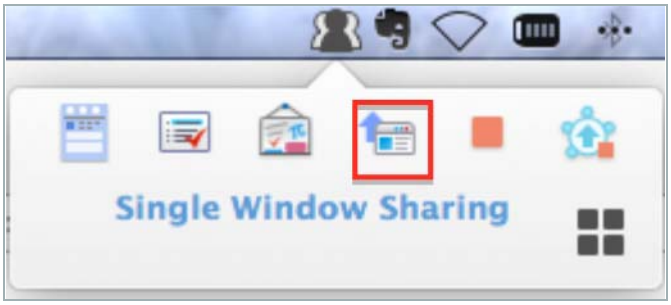
Sharing a Single Window

The Host can decide to share just a single window, rather than the whole desktop with meeting Participants.

To share a single window:

1 Click the Virtual Meeting icon on your pop-over icon panel.

2 Select the single window sharing icon.



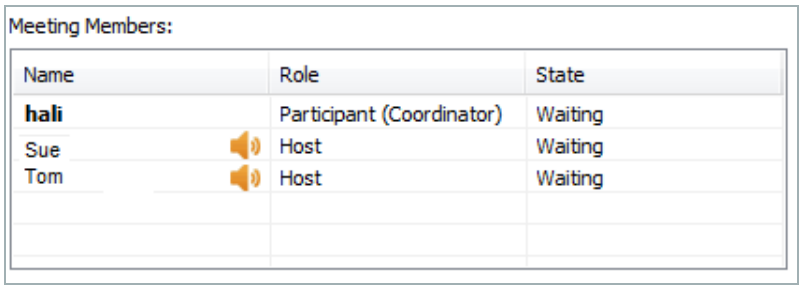
3 Select the window(s) to share from the Select Sharing Windows screen. If **Preview** is selected, you are able to view the window.

4 Click **OK** to finish sharing the window(s).

Starting Voice Conversation

The Coordinator can share one-way voice communication with meeting Participants. Only the Host can be heard. When voice communication is started an icon appears on the Meeting Members section of the Lobby window next to each meeting Participant.

Windows View:

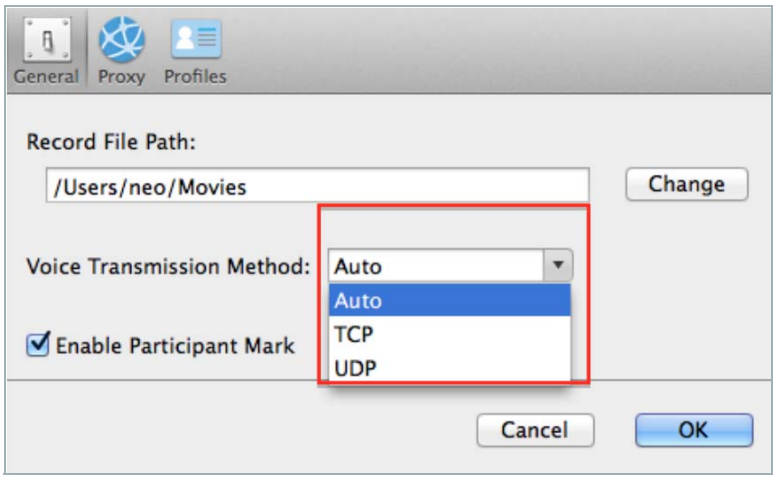


Mac OS X View:

There are three Voice Transmission methods to select from:

- TCP - The host uses the SSL tunnel to send voice data and all participants receive the voice data through the SSL tunnel. This method supports HTTP proxy.
- UDP - The host uses the DTLS tunnel to send voice data through the DLTS tunnel. This method does not support HTTP proxy.
- Auto - The host selects the voice transmission method based on the proxy settings.

For Mac OS X users, navigate to **Preferences** > **General** screen. Select the Voice Transmission Method from the drop-down list.



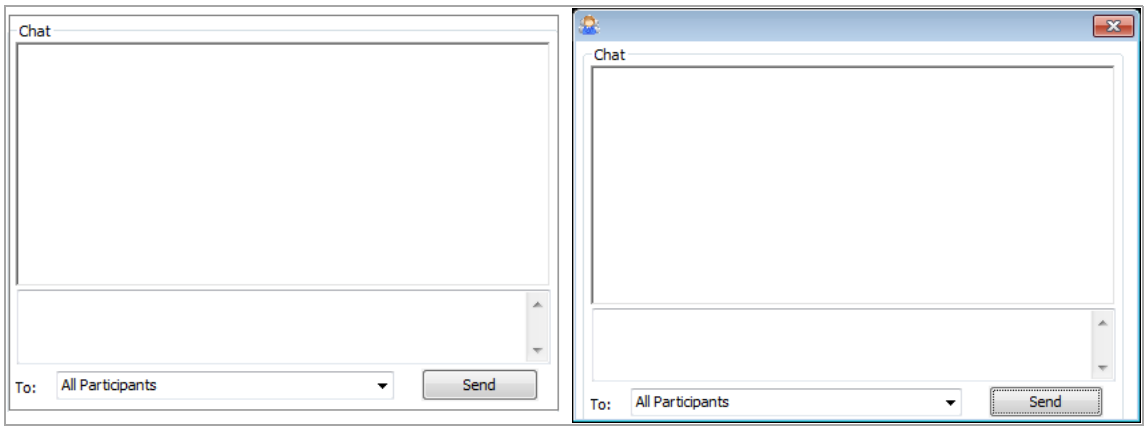
To use voice communication:

1 Click **Start Voice Conversation** to open voice communication with Participants in the meeting lobby.

2 When a voice conversation starts, **Start Voice Conversation** changes to **Stop Voice Conversation**. Click **Stop Voice Conversation** to end voice communication.

Text Chatting

Chat with all attendees in the meeting or have a private chat with one or more selected attendees, including View-only Participants.



If the lobby is hidden, click on the control menu after the meeting has started and the Host is sharing the screen. The chat window is displayed in a standalone chat window.

Recording a Meeting

Any meeting Participant can record the meeting screens in a .wmv file. The file is automatically named with the Host's name and the date and time the recording was started (for example, `Holi_EST_2013-2-12_09h47m43s.wmv`). The file location can be set on the Connection Settings window.

To record a meeting on Windows:

1 Click **Record** to start recording that displays recording controls at the bottom right of the window.

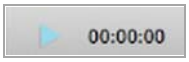
2 Use the recording controls to Start, Pause, and Stop the recording.

3 When recording starts, **Record** changes to **Stop Recording**.

4 Click **Stop Recording** to end recording.

To record a meeting on Mac OS X:

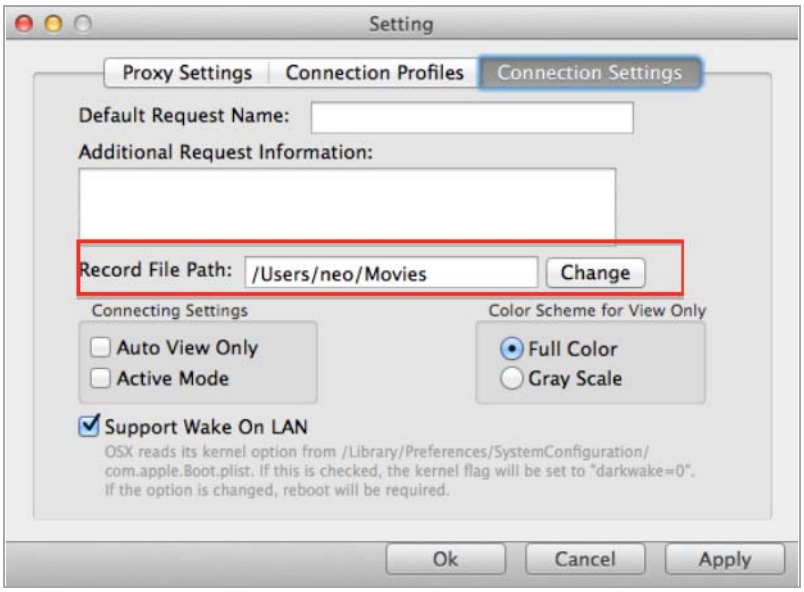
1 On the Technician view toolbar, click the Record icon . This opens the recording toolbar.



2 On the recording toolbar, click the Start Recording icon . The icon changes to indicate that a recording is in session.

3 To stop the recording, click the Stop Recording icon .

4 Configure the file path for the recorded session on the **Settings** > Connection Settings screen. Specify the **Record File Path**. The file is then saved as a .mov file.



5 Click **Apply** to save changes made.

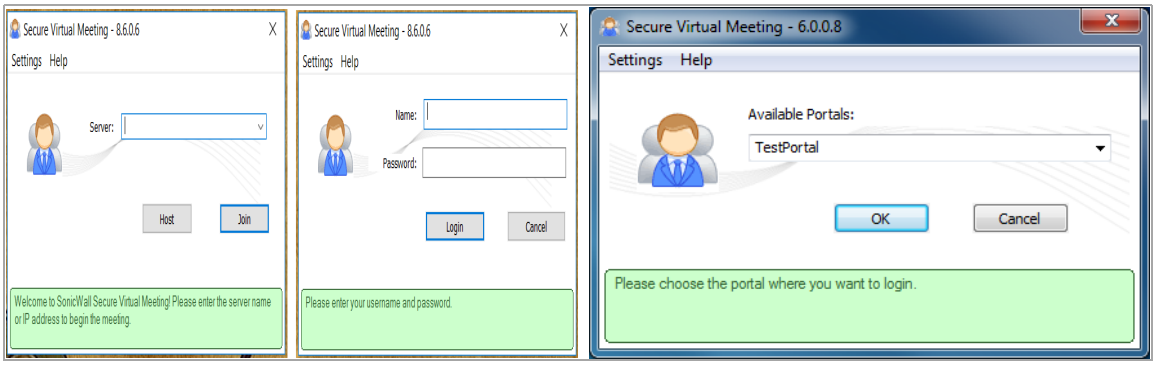
Participant Role

Participants can be designated as View-only Participants or regular Participants. View-only Participants enter and exit meetings like other Participants, but cannot complete most functions. However, they can be kicked out of meetings like other regular Participants. Regular Participants can also:

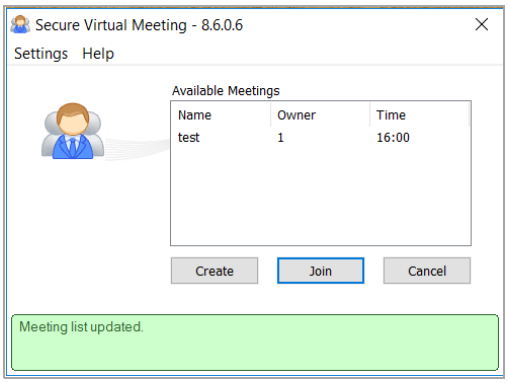
- Respond to polls
- Download shared files
- Text chat
- Request control of the Host keyboard and mouse
- Request to become the Host and share the Participant's desktop
- Become the Assistant
- Become a View-only Assistant

To join a meeting as a participant:

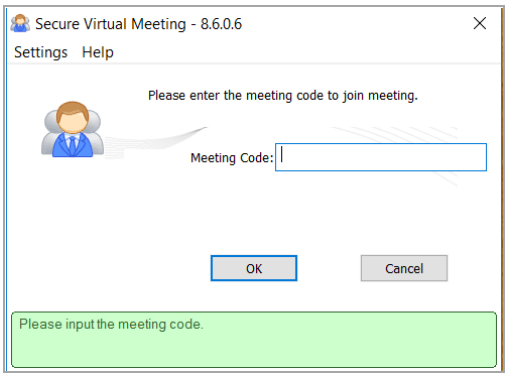
1 Click the link from the meeting email invitation or type the server name or IP address in the **Server** field of the Secure Virtual Meeting window.



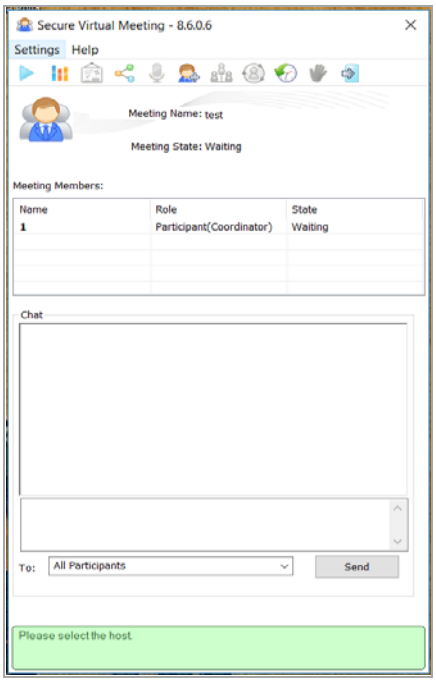
2 If necessary, select the proper meeting portal. All available meetings are displayed.



3 Select the meeting to join and click **Join**. The following prompt is displayed if you are required to enter a meeting code to join the meeting.



4 Enter the meeting code that was provided in the meeting email invitation and click **OK** to join the meeting. After joining the meeting, you are in the meeting lobby.



7

Using File Shares

File shares provide remote users with a secure HTML-based interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

The File Shares Applet mimics Windows Explorer navigation and provides functionality not available in HTML-based File Shares, including the ability to overwrite existing files and upload directories.

Topics:

- Using the File Shares Applet on page 117
- Using HTML-based File Shares on page 119

Using the File Shares Applet

The File Shares Applet has a similar look and feel to the Windows Explorer tool, featuring drag-and-drop and multiple file selection capabilities. It also provides the user the ability to set up bookmarks to quickly navigate through networks from the portal level. This feature saves time lost moving through network and server paths. With the help of the HTTPS protocol, the applet securely transfers encrypted files and information to and from the SMA/SRA appliance. The appliance communicates this data to the individual machines on the remote network.

Topics:

- User Prerequisites on page 117
- Configuration Overview on page 118

User Prerequisites

Supported web browsers for Secure Mobile Access is listed in Browser requirements on page 10. For optimal performance, use the most recent supported version shown in this list.

The Administrator must enable the File Shares Applet for users to use it.

There must be a computer with open access for the Secure Mobile Access File Shares Applet to log in to. 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.

Configuration Overview

The File Shares Applet is easy and intuitive to use. User should be aware of its functions and limitations. Setting up bookmarks and the browser interface are covered in this section, along with an overview of the browser and sample use cases.

Topics:

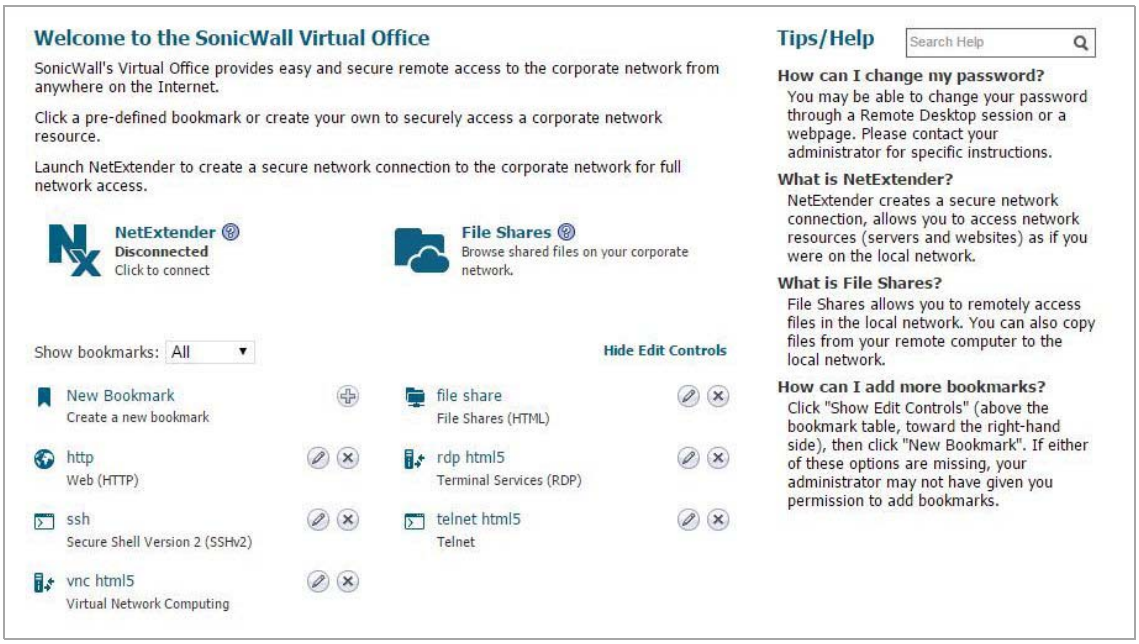
- Setting up Bookmarks on page 118
- Using HTML-based File Shares on page 119

Setting up Bookmarks

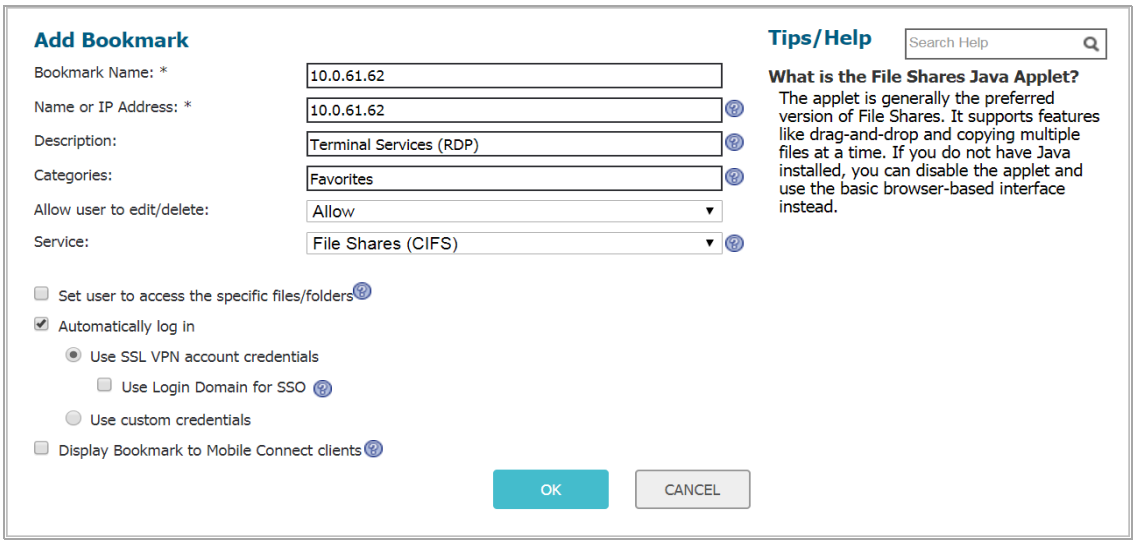
Bookmarks can be set up for folders and for files. A file bookmark does not launch the Applet, but instead downloads and launches the file directly. Bookmarks must be enabled by the Administrator.

To set up bookmarks from the Virtual Office Portal:

1. Open a web browser and log in to the Secure Mobile Access Virtual Office interface by typing the URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** drop-down. Click **Login**.
2. Click the **Show Edit Controls** link in the middle of the portal page.
3. Click the **New Bookmark** tab in the portal page.



4 The Add/Edit Bookmark screen displays. Enter a friendly name for the bookmark in the **Bookmark Name** field.



5 Enter the IP address and file directory path to the File Share in the **Name or IP Address** field.

NOTE: The **Name or IP Address** field must be to a file directory and end with a / or \ character.

6 In the **Service** drop-down menu, select the **File Shares (CIFS)** option.

7 Optionally, select **Automatically log in** to log in to this file share using either your Secure Mobile Access credentials or by specifying custom credentials.

8 Click **Add**.

Bookmarks serve as useful shortcuts to quickly access different network locations. Bookmarks can also be set up from the File Shares Browser, either by clicking **Bookmark**, or using the bookmark option from the right-click menu.

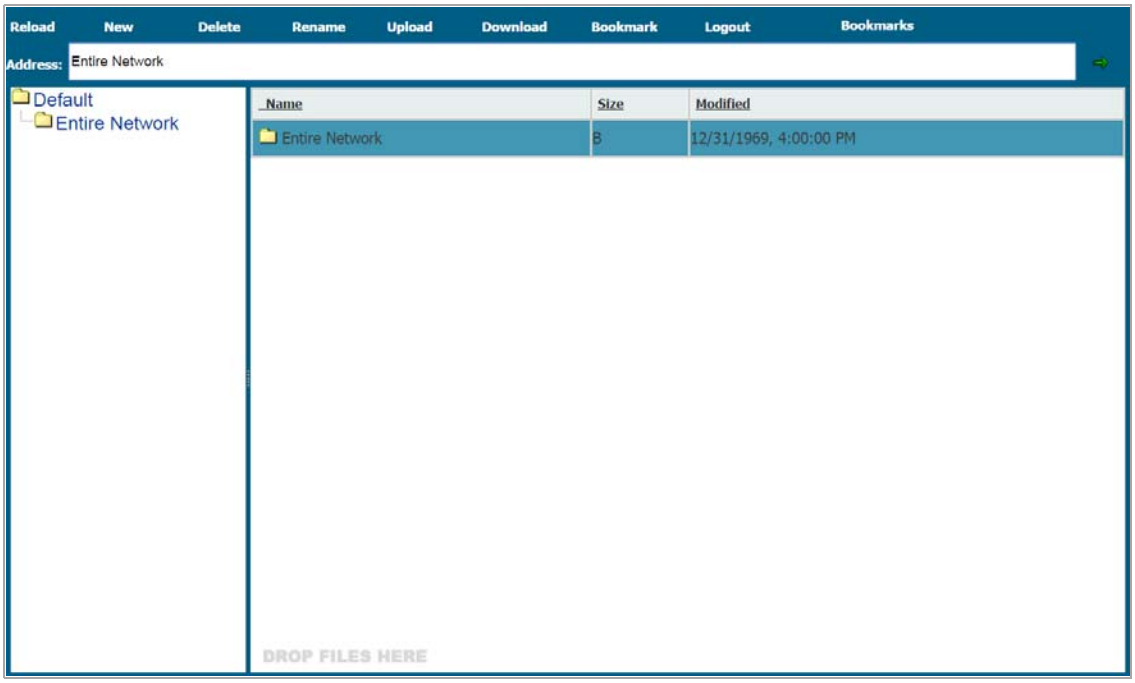
Using HTML-based File Shares

File shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

NOTE: The server can be specified either by name or by IP address, for example, **\\moosedc** or **\\10.50.165.2**. For names to work, it is necessary that DNS and/or WINS be properly configured by the Administrator on the SMA/SRA appliance to be able to resolve host names.

To create a file share:

1 Click **File Shares**. Virtual Office displays a dialog box that provides a hot link to a login prompt.



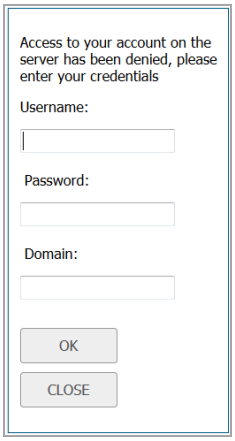
NOTE: Pop-up window blockers might prevent File Shares from functioning properly. Configure your browser to allow pop-up windows on the Secure Mobile Access portal site.

2 To specify a new share path (as an example, **\\moosedc**) in the **Address** field. You need to precede the share name with two back slashes. For example: **\\file-directory01.example.com**.

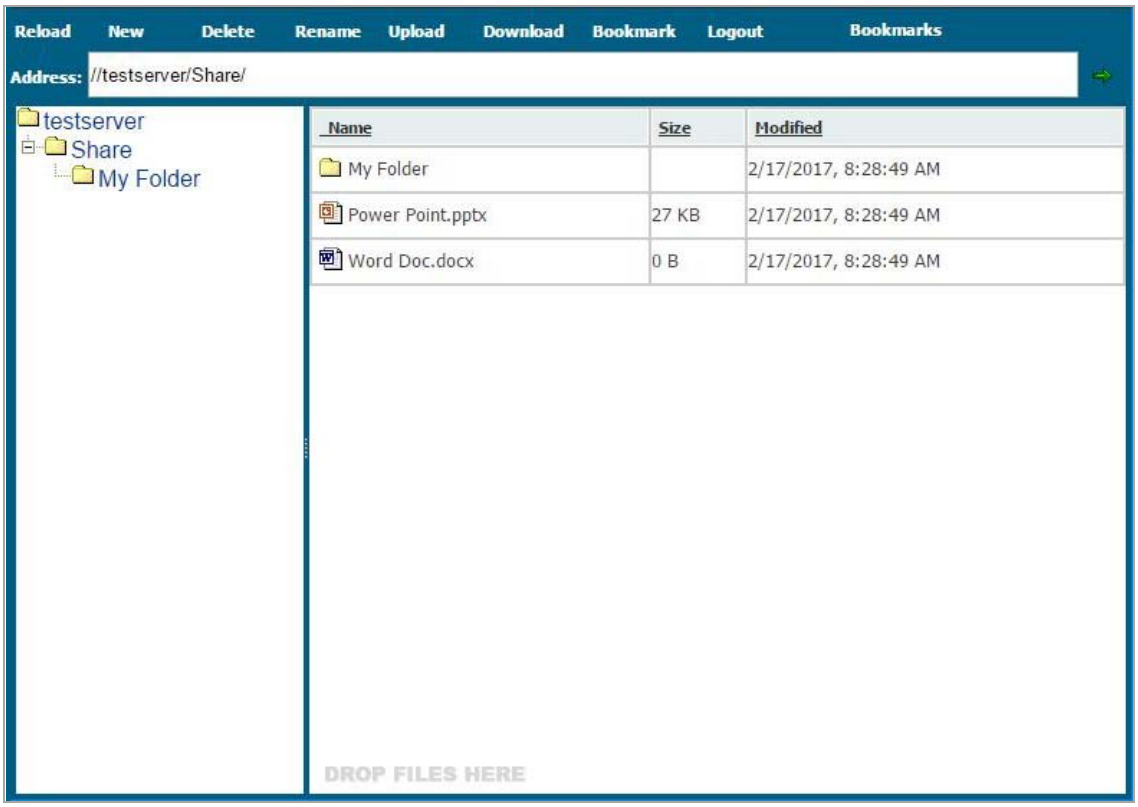
3 To connect to a pre-existing file share, click the **Login to Server** link next to the file share name.

4 Click the **go** prompt to display the **Enter Network Password** dialog box.

5 Type a valid username in the User Name field and a valid password in the Password field and click **Login**.



6 Virtual Office displays the home File Share screen that you have specified, displaying folders on the network to which you can navigate.



Below, the File Share Controls table describes the controls at the top of the File Share window.

File Share Controls

Button	Description
Back	Navigate to the previous File Share location.
Forward	Navigates forward to the previous File Share location after you have pressed **Back**.
Reload	Reloads the current folder to display any changes.
Up	Navigates
Delete	Deletes the selected folder or folders. Note that only empty folders can be deleted. If there are files in the folder, an error message is displayed. Delete all files out of the folder and then delete the folder.
Rename	Renames the selected folders and files. Choose items by selecting the check box next to their name under the **Select** column.
Bookmark	Creates a new bookmark to the current File Share location.
Logout	Logout of the File Share service.

7 You can now navigate the folders and files in the File Share as you would through Windows Explorer or other file management systems.

8 To add a new folder in the current File Share location, type the name of the folder in the **Add New Folder:** field and click **Submit**.

9 To add a file in the current File Share location, click **Browse...**. Navigate to the location of the file on your computer in the **Choose file** window that opens, select the file and click **OK**, and then click **Submit** in the File Share window.

8

Managing Bookmarks

Bookmarks are objects that enable you to connect to a location or application conveniently and quickly. The Virtual Office Bookmark system allows bookmarks to be created at the group and user levels. The Administrator can create both group and user bookmarks which applies to applicable users while individual users can create only personal (user-level) bookmarks.

Because bookmarks are stored within the security appliance's local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local groups and users (LocalDomain), this is automated since the Administrator must manually define the groups and users on the device. Similarly, when working with external groups (not LocalDomain), the correlation is automated since creating an external domain creates a corresponding local group.

However, when working with external users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SMA/SRA appliance's configuration files. The need to store bookmarks on the SMA/SRA appliance itself is because LDAP, RADIUS, and NT authentication external domains do not provide a direct facility to store such information as bookmarks.

Rather than requiring Administrators to manually create local users for external domain users wishing to use personal bookmarks, Secure Mobile Access automatically creates a corresponding local user entity when an external domain user logs in to the Virtual Office.

The following sections describe basic bookmark tasks:

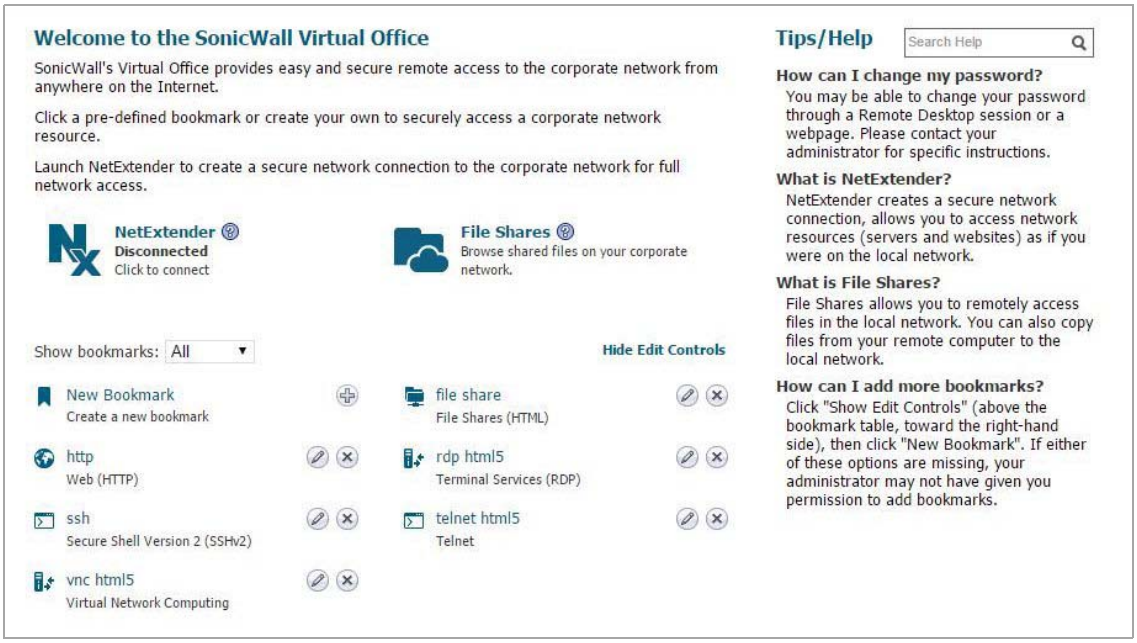
- Adding Bookmarks on page 123
- Editing Bookmarks on page 133
- Removing Bookmarks on page 134
- Using Bookmarks on page 134

Adding Bookmarks

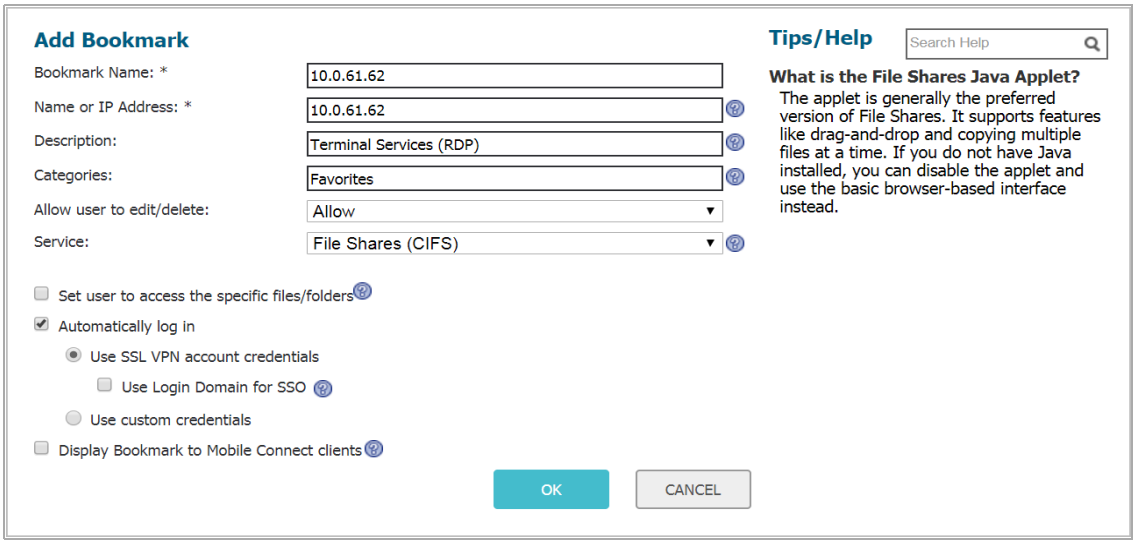
Bookmarks provide a convenient way for you to access Web, FTP, or other services on the remote network that you connect to frequently.

To define bookmarks:

1 In the Virtual Office window at the top of the bookmarks table, click **Show Edit Controls** and then click **New Bookmark**.



2 In the Add Bookmark screen, enter a descriptive name in the **Bookmark Name** field.



3 Enter the domain name, IP address, or IPv6 address of a host machine on the LAN in the **Name or IP Address** field. IPv6 addresses should be enclosed in brackets (meaning the [and] symbols). You can also enter the wildcard variable **%USERNAME%** to display the current user name. Variables are case-sensitive.

4 In the **Description** field, optionally enter a friendly description to be displayed in the bookmark table.

5 In the **Categories** field, optionally enter a comma-separated list of tabs where this bookmark should appear. Standard tabs (Desktop, Web, Files, Terminal, and Mobile) do not need to be specified. For example, Favorites, Tab 1, Tab 2.

6 Select the user permissions level from the **Allow user to edit/delete** drop-down list. You can select **Use user policy**, **Allow**, or **Deny**.

7 Select the service type in the **Service** drop-down list. You can select from the following services:

- Terminal Services (RDP)
- Virtual Network Computing (VNC)
- Citrix Portal (Citrix)
- Web (HTTP)
- Secure Web (HTTPS)
- External Web Site
- Mobile Connect
- File Shares (CIFS)
- File Transfer Protocol (FTP)
- SSH File Transfer Protocol (SFTP)
- Telnet
- Secure Shell version 2 (SSHv2)

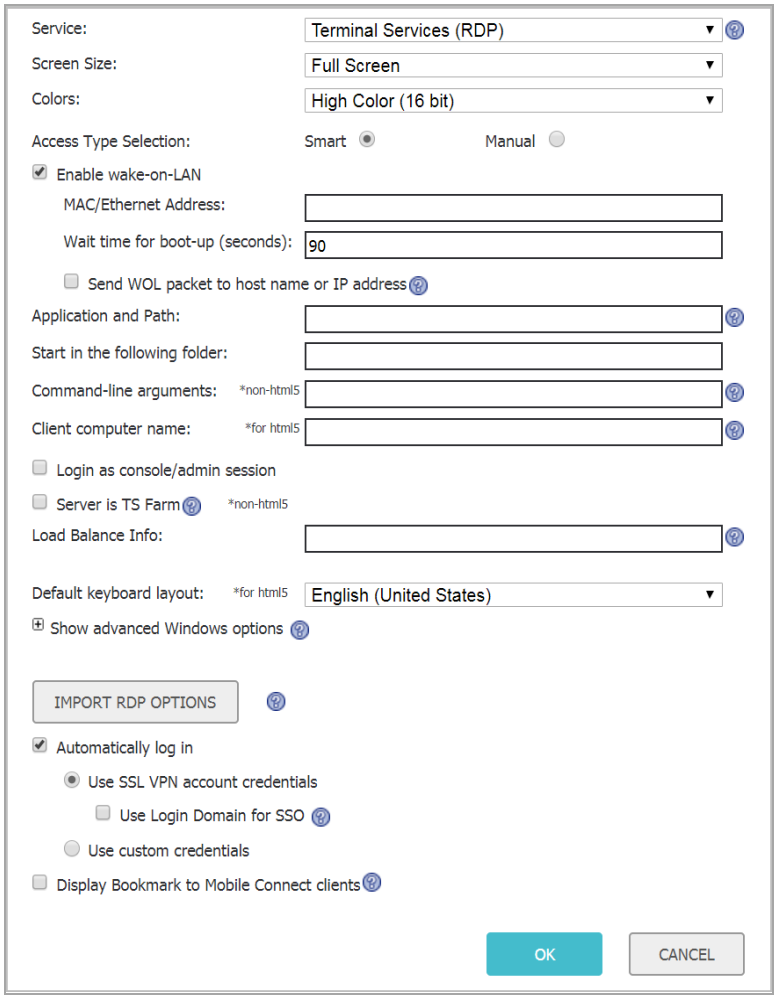
The following sections provide additional details about adding the different types of bookmarks:

- RDP Bookmarks on page 126
- Citrix Bookmarks on page 130
- Web Bookmarks on page 132
- Mobile Connect Bookmarks on page 133
- FTP Bookmarks on page 133
- SSHv2 Bookmarks on page 133

After the configuration has been updated, the new bookmark is displayed in the Virtual Office Bookmarks table. Click a bookmark description to go to the bookmark location that you have defined.

RDP Bookmarks

RDP bookmarks offer several features that are not available in other bookmarks.



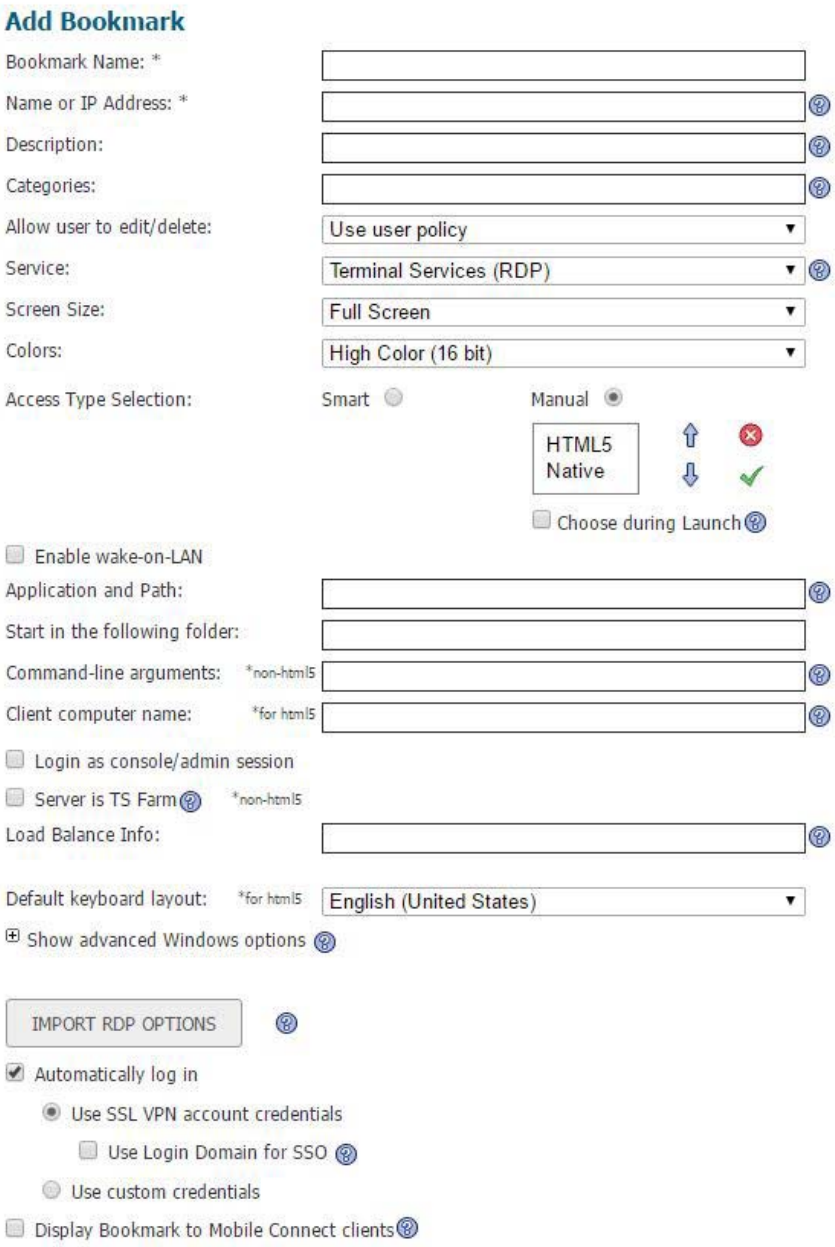
For information about configuring the remote computer to allow RDP access, see:

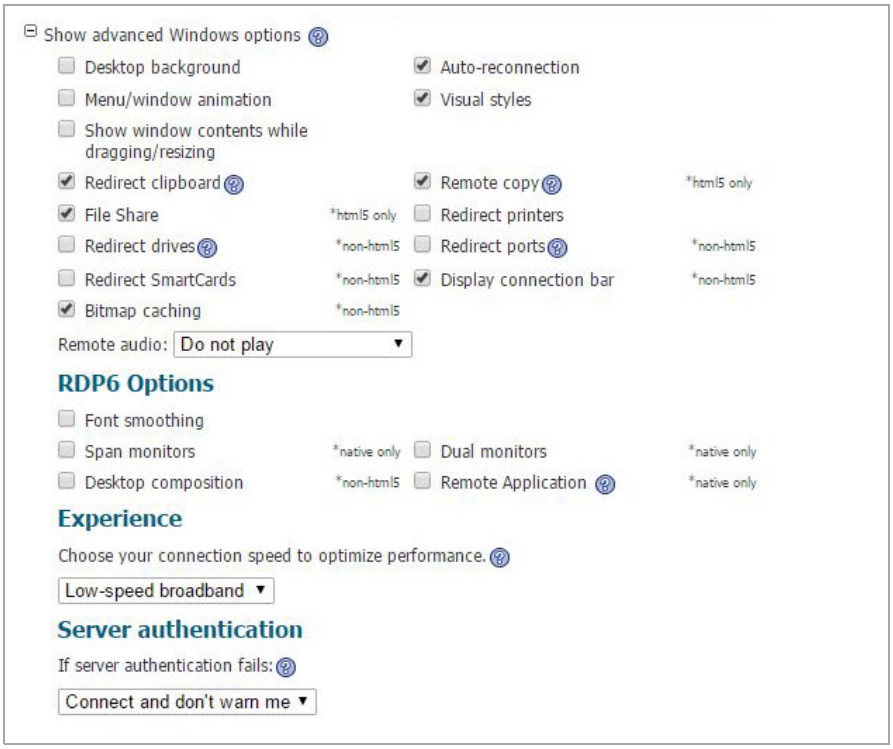
- Determining the Remote Computer's Full Name or IP Address on page 129
- Configuring Remote Desktop Access on the Remote Computer on page 130

To create an RDP bookmark:

1. Enter the desired **Bookmark Name**.
2. Enter the **Name or IP Address** of the resource you are trying to reach. You can also use an IPv6 address.
3. In the **Description** field, type a brief description of the bookmark.
4. In the **Tabs** field, create a comma-separate list of tabs showing where the bookmark should be displayed.
5. Select **Terminal Services (RDP)** from the **Services** list. Standard tabs (Desktop, Web, Files, Terminal, Mobile) do not need to be included.

6 Continue to configure the RDP Bookmark. the RDP Bookmark Options table provides information about the settings.





RDP Bookmark Options

Option	Usage
Screen Size	Select the default screen size to be used when users execute this bookmark. It is advised that you select a size equal to or smaller than your current desktop screen size. RDP bookmarks also have a **full-screen** option that displays the RDP window in full screen mode. To toggle from the RDP window back to your desktop, press **Alt-Tab**.
Colors	Select the default color depth to be used when users execute this bookmark.
Access Type Selection	• **Smart**: Allows the firmware to decide which mode to launch on the client. When creating a new unified bookmark, Smart is selected by default. Auto-detection is processed using bookmark-specific default modes while launching the bookmark. • **Manual**: Provides options to configure the modes, their priorities, and the choose method. At least one mode should be enabled in the selection box.
Enable wake-on-LAN	Select this option to send WoL packets to the host. This option also allows entering one or more **Mac/Ethernet Addresses** (separated by spaces) for the machines to wake and the desired **Wait time for boot-up** before cancelling the WoL operation. To send the WoL packet to the hostname or IP of this bookmark, select the **Send WOL packet to bookmark host Name or IP address** check box, this option can be applied in tandem with a Mac address.
Application and Path	To have the RDP session launch an application when the bookmark is initiated, enter the path to the application in the **Application and Path (optional)**: field. For example, C:\Program Files\Example\app.exe (optional).
Start in the following folder	Enter the local folder to execute application commands in (optional).

RDP Bookmark Options (Continued)

Option	Usage
Command-line arguments	Type any command-line arguments required to access the remote application.
Client computer name	Type the client computer name.
Login as console/admin session	Select this option to enable console and admin commands on login.
Server is TS Farm	Select this option if users connect to a TS Farm or load balanced server. You might need to disable interactive login for this option to work properly.
Load Balance Info:	Enter the Terminal Services Broker information in the L**oad Balance Info** box, such as `tsv://MS Terminal Services Plugin.1.SSLVPN`. Maximum length is 1024 characters. For the bookmark with complex options (like RDP), options are mixed from all the modes and distinguished with tips like *non-html5, or *for html5.
Default keyboard layout	For *RDP - HTML5*, select the Default Language from the drop-down menu.
Show advanced Windows options	Optionally expand **Show windows advanced options** and select any of the redirect check boxes, as well as any of the additional listed features for use in this bookmark session. You can select any of the following options as well: **Dual monitors, Span monitors, Font smoothing, Desktop composition, and Remote Application**.
Import RDP Options	When the RDP file finishes downloading, open it with a text editor (such as Notepad) and select the entire file content. Copy the content and paste the text into the text field in Import RDP Options. Click **OK**. The feature selects the support options to import into the bookmark.
Automatically log in	Select this option and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark.
Display Bookmark to Mobile Connect clients	Select this option to display bookmarks to Mobile Connect clients running Mobile Connect 2.0 or higher. Some devices might require supported third-party applications for this feature to work properly.

7 When you are finished. Click **Add** to add this bookmark to your Virtual Office list.

Determining the Remote Computer's Full Name or IP Address

To determine the full name of the computer to which the RDP bookmark is pointing:

1 Right click the **My Computer** icon on the desktop of the remote computer, and select **Properties**.

2 Click the **Remote** tab.

3 The full computer name is listed under Remote Desktop.

To determine the IP address of your computer.

1 In the Windows **Start** menu on the remote computer, navigate to **Run...**

2 Type **cmd** to open the command interpreter and click **OK**.

3 Type **ipconfig**. The IP address of your computer is displayed.

Configuring Remote Desktop Access on the Remote Computer

To allow remote desktop access to the computer that is the target of the RDP bookmark:

1 Right click the **My Computer icon on the desktop, and select Properties.**

2 Click the **Remote** tab.

3 Under Remote Desktop, select the check box for **Allow connections from computers running any version of Remote Desktop (less secure)**. By default, RDP has Transport Layer Security (TLS) enabled.

To use Network Level Authentication (NLA), which is a security enhancement for computers using RDP bookmarks, click the check box for **Allow connections only from computer running Remote Desktop with Network Level Authentication (more secure)**.

4 Click **OK**.

Citrix Bookmarks

For Citrix bookmarks, you can select the following options:

- The SMA/SRA appliance always performs the Citrix client detection when using Citrix Bookmarks. Click the **Disable client detection by Citrix server** check box to disable this feature when using Citrix Bookmarks. Note that this feature is compatible with Citrix XenAPP 5.0 or later.
- Select the **HTTPS Mode** check box to use a secure Citrix connection.
- Select an **Access Type Selection**. **Smart** or **Manual**.
  - **Smart**: Allows the firmware to decide which mode to launch on the client.

When creating a new unified bookmark, **Smart** is selected by default. Auto-detection is processed using bookmark-specific default modes while launching the bookmark.

  - **Manual**: Provides options to configure the modes, their priorities, and the choose method. At least one mode should be enabled in the selection box.

The launch sequence is as follows: **HTML5** and **Native**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection. Both should be installed before choosing **Native**. If you choose to run as **HTML5**, the Citrix HTML5 client is used to view the Citrix3 backend host.

The **up** and **down** arrows are used to adjust the launch priority. Fork and tick are used to disable or enable the modes. Disabled modes are put at the bottom of the list with a gray font color.

The **Choose during Launch** option is not enabled by default under the **Manual** mode. In this setting, while launching the bookmark, the first available mode in the configured list is run at once after auto-detection.

After the **Choose during Launch** option is enabled, while launching the unified bookmark, if there are multiple modes available for the client, a menu is provided from which you can choose within

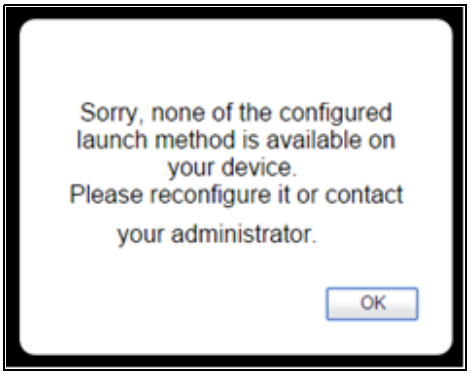
a five second count-down. When only one mode is available, the bookmark is also run immediately.

If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

That means, when next launching the bookmark, the remembered mode is run directly within two seconds. Clicking anywhere in the HTML can 'forget' the remembered mode so you can re-choose.

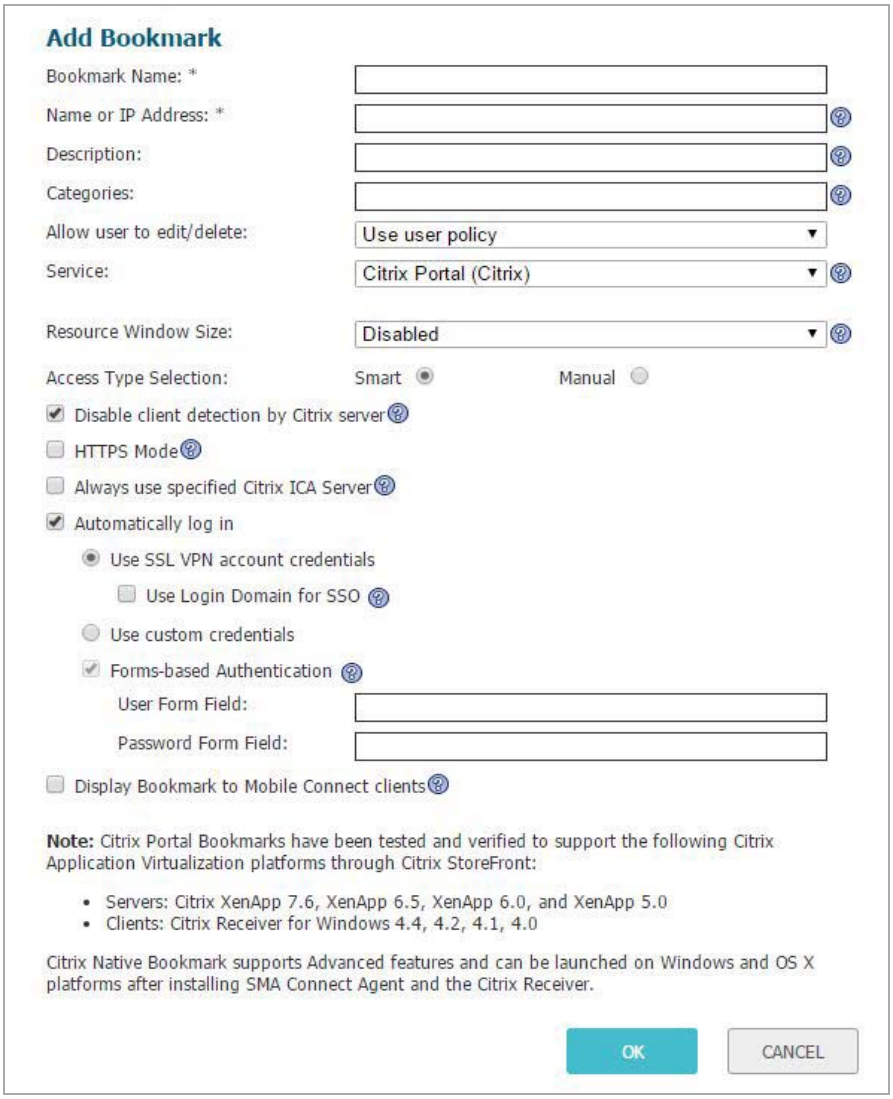
Editing or deleting the bookmark in the same browser can also reset the remembered mode.

When no modes are able to run on the client with the configuration, the following notice appears.



- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.

- Select **Always use specified Citrix ICA Server** to explicitly specify the Citrix ICA Server Address for the Citrix ICA Session. By default, the Bookmark uses the information provided in the ICA configuration on the Citrix server.



Web Bookmarks

For HTTP(S) bookmarks, you can select **Use SSL-VPN account credentials to log in** or configure custom credentials for use with Single Sign-On. To disable the use of SSO, clear the **Automatically log in** check box. Select the Forms-based Authentication check box to use this method, and then fill in the following fields that are exposed:

- Configure the **User Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing User Name in the Login form, for example:

  <input type=text name='userid'>

- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:

  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>

For External Web Site bookmarks, select **HTTPS Mode** to encrypt Web communication with SSL. External Web Site bookmarks are used to access an offloaded Web site or portal using a bookmark. Select **Disable security warning** if you do not want a security warning dialog box to be displayed when a user clicks this bookmark. If left cleared, the warning dialog allows the user to select a "Do not show this warning again" option if the user has permissions to edit this bookmark (set above).

For more information about offloaded applications, see the Application Offloading section in the *SonicWall Secure Mobile Access Administration* documentation.

Mobile Connect Bookmarks

The Mobile Connect bookmark allows a custom bookmark to be defined for display in Mobile Connect after the user is connected. This bookmark is meant to support any third-party app, whether an in-house app or a public app in the App Store or Google Play. The bookmark also enables calling third-party apps that have defined a custom URL scheme, for example 'comgoogleearth://' for Google Earth. The Mobile Connect bookmark is only available for edit from normal browsers and is intended for use only on mobile devices.

NOTE: The Mobile Connect bookmark might also be used for 'http://' or 'https://' URL schemes, however, SonicWall recommends using HTTP or HTTPS bookmarks for these schemes.

FTP Bookmarks

For FTP bookmarks, click **Show advance server configuration** to select the **Character Encoding**. You can also select **Use SSL-VPN account credentials to log in** or configure custom credentials for use with Single Sign-On. To disable the use of SSO, clear the **Automatically log in** check box.

SSHv2 Bookmarks

For SSHv2 bookmarks, you must have SUN JRE 1.6.0_10 or higher and must be connecting to a server that supports SSHv2. The **Access Type Selection** option is available for use here. There are also options to **Automatically accept host key** and to **Bypass username**. The bypass option should only be used for SSHv2 servers that do not require authentication in the initial connection session (such as SonicWall security appliances).

Editing Bookmarks

You can change the IP address, domain name, or IPv6 address as well as the service and other settings associated with an existing bookmark.

NOTE: Only user-created Bookmarks can be edited or deleted by the user. Global or Group Bookmarks pre-defined by the Administrator cannot be edited or deleted.

To edit a bookmark to change its name or associated IP address:

1 Identify a bookmark in the Virtual Office Bookmarks list for which you want to change an IP address or domain name or other settings.

2 In the Virtual Office Bookmarks list, click the Configure icon for an existing bookmark. The **Edit Bookmark** dialog box displays.

3 To change the bookmark name, domain name or IP address of the bookmark, edit the names in the **Bookmark Name** or **Name or IP Address** fields.

4 To change the service, select a new **Service** from the drop-down menu.

5 Optionally change other settings specific to the **Service** type.

6 Optionally enable or disable the **Automatically log in** setting, or change the credentials selection.

7 Click **Apply**. The Virtual Office home page displays with the new IP address or domain name.

Removing Bookmarks

To remove a bookmark:

1 Identify a bookmark in the Virtual Office Bookmarks list that you want to remove.

2 In the Virtual Office Bookmarks list, click the delete icon for the bookmark you want to remove. The bookmark disappears from the list.

Using Bookmarks

The following sections describe how to use the various types of bookmarks:

- Using Remote Desktop Bookmarks on page 134
- Using VNC Bookmarks on page 137
- Using Citrix Bookmarks on page 138
- Using Web Bookmarks on page 139
- Using Mobile Connect Bookmarks on page 139
- Using File Share Bookmarks on page 140
- Using FTP Bookmarks on page 140
- Using Telnet Bookmarks on page 143
- Using SSHv2 Bookmarks on page 143
- Global Bookmark Single Sign-On Options on page 145
- Per-Bookmark Single Sign-On Options on page 145

Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. Secure Mobile Access supports the RDP5 standard with ActiveX and HTML5 clients. RDP5 ActiveX can only be used through Internet Explorer. The basic functionality of the two clients is the same; however, the HTML5 client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect Printers
- Redirect Ports

- Redirect Drives
- Redirect SmartCards
- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Bitmap caching
- Menu/window animation
- Visual styles
- Window drag

If the HTML5 client application is RDP 6, it also supports:

- Dual monitors
- Span monitors
- Font smoothing
- Desktop composition
- Remote Application

Secure Mobile Access also supports the Terminal Services (Using Tunnel) bookmark that uses the NetExtender Client to tunnel RDP data, and does not need Browser Plug-ins to function. This bookmark should be used if your system is experiencing issues with RDP disconnect/reconnect that commonly occur when using the Windows 10 OS.

This bookmark works just like the existing RDP bookmarks, and the bookmark setting page is same as RDP ActiveX bookmark. All the advanced options are exactly same, but this bookmark starts the NetExtender Client first before launching the native RDC client. So this bookmark needs the NetExtender connection allowed to the portal.

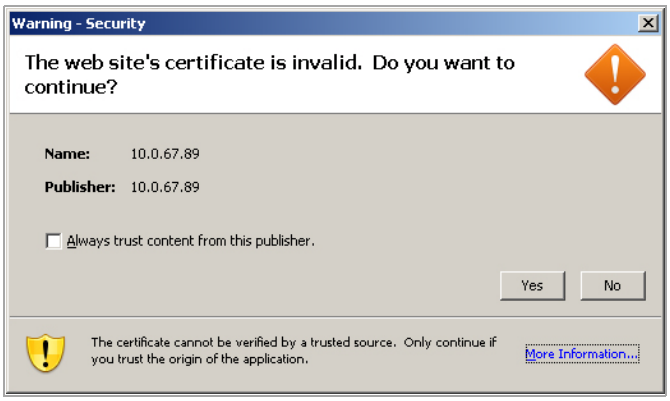
This bookmark would start the NetExtender connection if it is not connected, and add host route to the NetExtender adapter. If the NetExtender connection is done by this RDP bookmark, after the RDP connection is closed, it need to auto disconnect the NetExtender connection.

NOTE: RDP bookmarks can use a port designation if the service is not running on the default port.

TIP: To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you might simply close the remote desktop window.

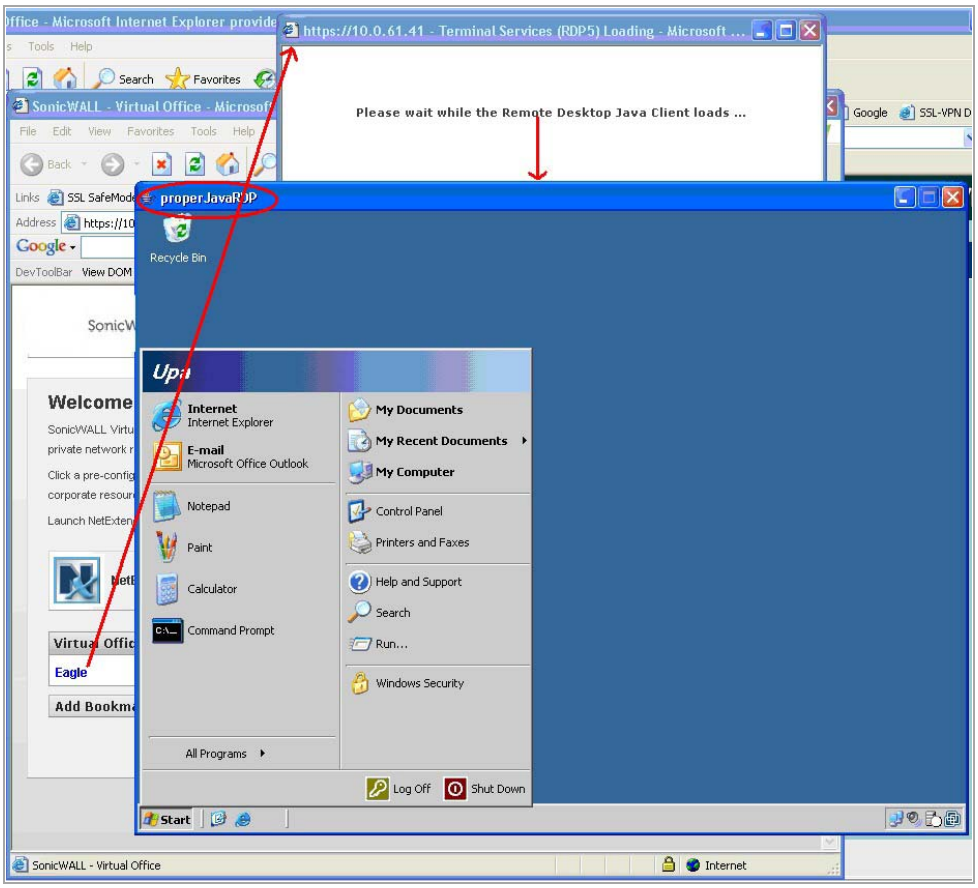
To access a system with an RDP bookmark:

1 Click the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **Ok**.



2 Enter your username and password at the login screen and select the proper domain name from the drop-down menu.

3 A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.



For information on configuring options for RDP bookmarks, see Web Bookmarks on page 132.

Using VNC Bookmarks

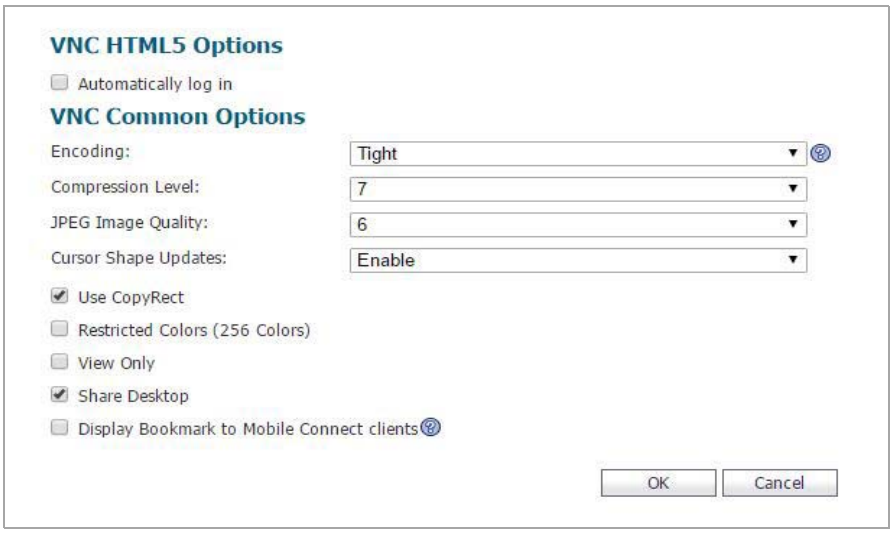
To use a VNC bookmark:

1 Click the VNC bookmark. The following window is displayed while the VNC client is loading.

NOTE: VNC can have a port designation if the service is running on a different port.

2 When the VNC client has loaded, you are prompted to enter your password in the **VNC Authentication** window.

3 VNC options must be configured by the administrator. Contact your administrator if you do not have permission to edit the bookmark options.



Below, the VNC Options table describes the options that the administrator can configure for VNC.

VNC Options

Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but might be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG Image Quality	6	This cannot be modified.
Cursor Shape Updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable** but the remote cursor is not visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted Colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors might look very inaccurate.
View Only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window is silently ignored and is not passed to the remote side.
Share Desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No** then an existing user session ends when a new user accesses the desktop.
Display Bookmark to Mobile Connect clients	Yes	Select the **Display Bookmark to Mobile Connect clients** check box to enable bookmark viewing on Mobile Connect clients. Mobile Connect must be running version 2.0 or newer to view and access this bookmark.

Using Citrix Bookmarks

Citrix is a remote access, application sharing service, similar to RDP. It enables users to remotely access files and applications on a central computer over a secure connection. There are two types of Citrix bookmarks:

- Native

- HTML5

Using Web Bookmarks

Web bookmarks are also known as HTTP or HTTPS bookmarks.

HTTP & HTTPS Bookmarks have been tested and verified to support the following web applications:

- Microsoft Outlook Web Access 2013, Outlook Web Access 2010, and Outlook Web Access 2007
- Windows SharePoint 2007, and Windows SharePoint Services 3.0

  NOTE: The client integrated features of SharePoint are not supported.

- Lotus Domino Web Access 8.0.1, 8.5.1 and 8.5.2
- Novell Groupwise Web Access 7.0

Other applications might work, but there might be problems accessing pages that are malformed, have advanced HTML features, use an unsupported authentication method (for example, Windows Integrated Authentication) and URLs that are embedded in Macromedia Flash, Java or ActiveX. If a web application does not work with a HTTP or HTTPS Bookmark, contact your Administrator.

To use a web bookmark:

1 Click the HTTP or HTTPS bookmark.

  NOTE: HTTP bookmarks can have a port designation and a path.

2 A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.

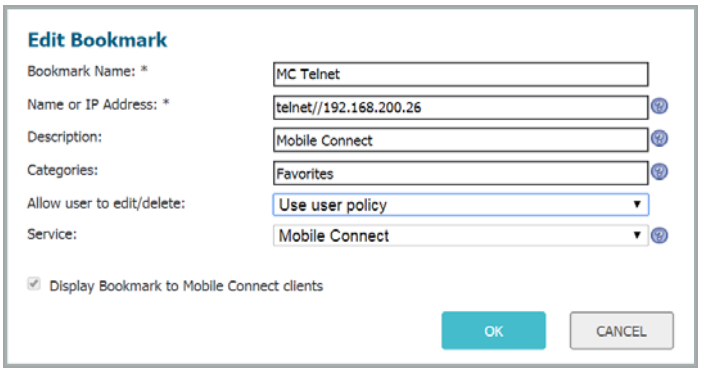
Using Mobile Connect Bookmarks

To use a Mobile Connect bookmark:

1 Click the Mobile Connect bookmark.

2 Enter the **Bookmark Name** and the **Name or IP Address**. The Name or IP Address field is the custom URL scheme.

3 Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients. Click **OK**.



After the Mobile Connect bookmark on the Secure Mobile Access is successfully configured, the bookmark displays on your mobile device:

Using File Share Bookmarks

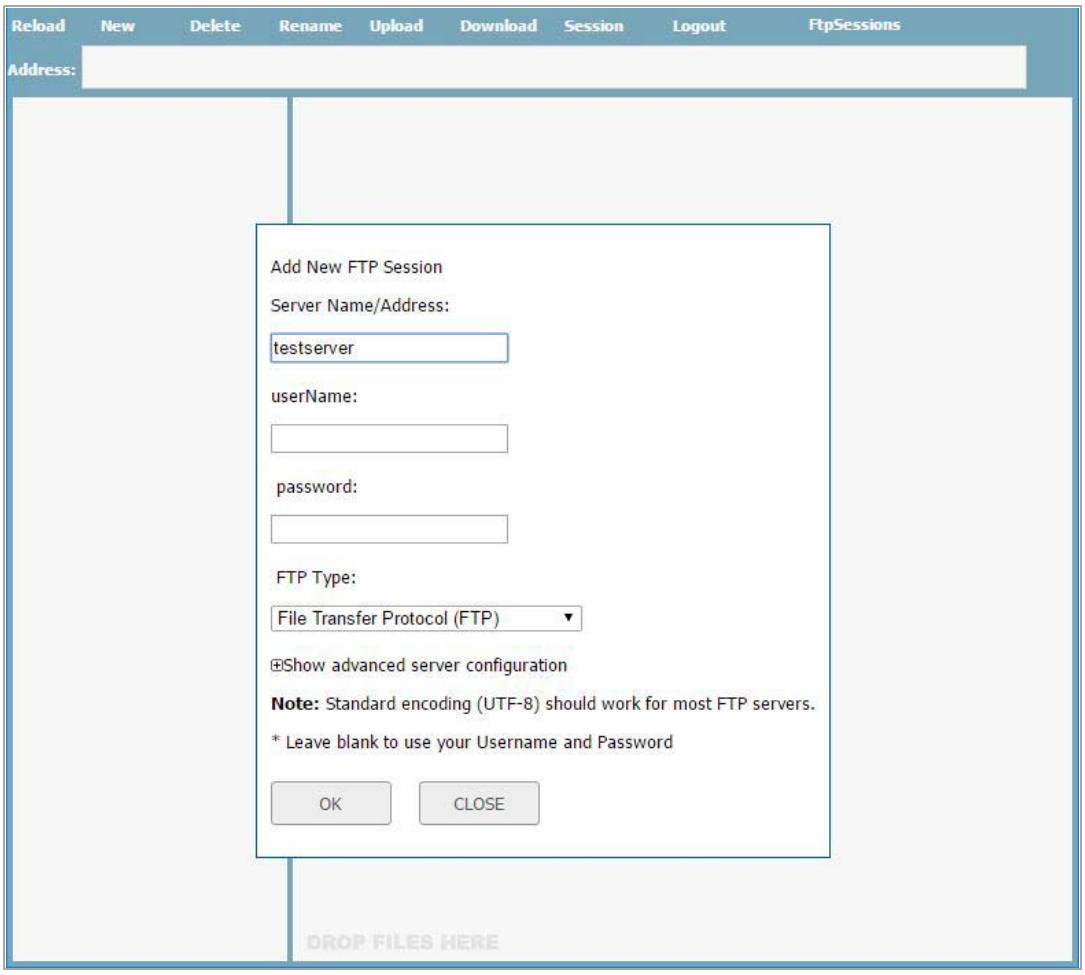
For information on using File Share (CIFS) bookmarks, see Using HTML-based File Shares on page 119.

Using FTP Bookmarks

FTP bookmarks can use a port designation if the service is not running on the default port.

To use an FTP bookmark:

1 Click the **FTP** bookmark. The **FTP Session** dialog box displays.

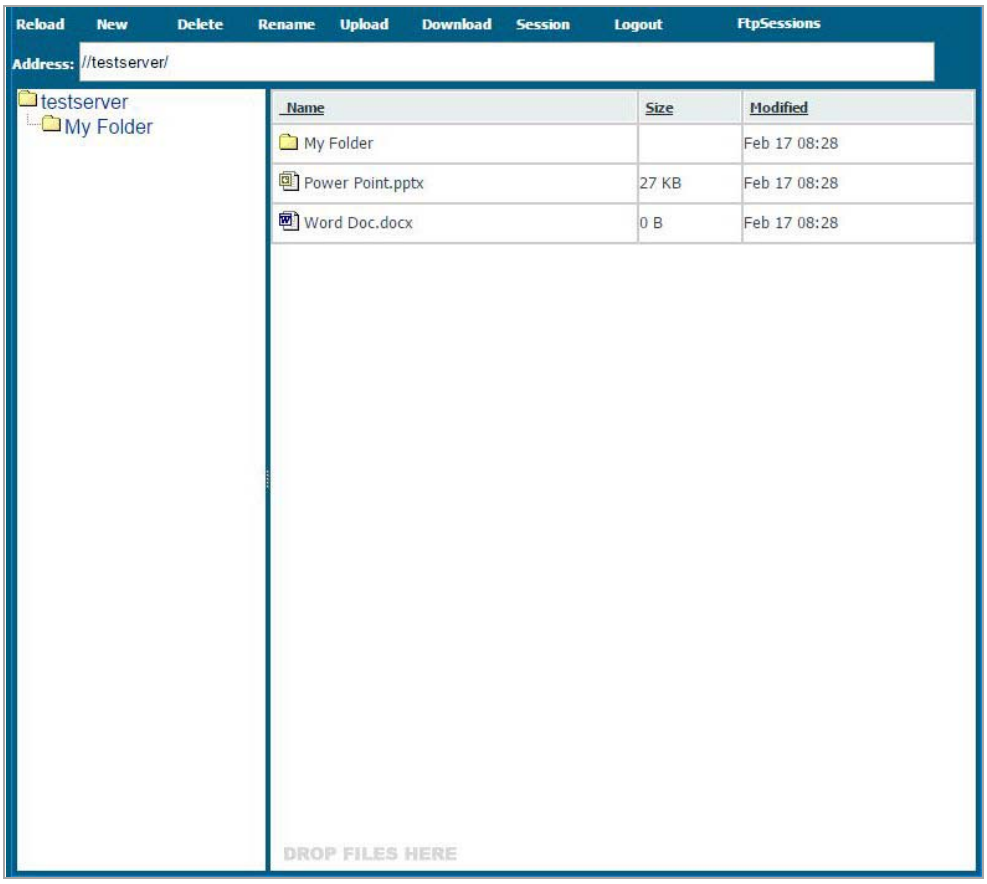


2 If the server name or IP address is not displayed, enter it in the **Server Name/Address** field.

3 Enter your username and password. If you want to use your Virtual Office username and password, simply leave the fields blank.

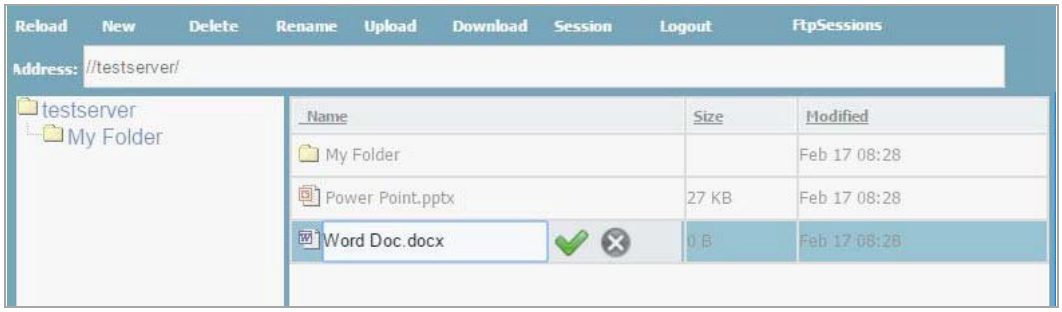
4 Optionally expand **Show advanced server configuration** and select the desired settings.

5 Click **OK**. An FTP session displays.

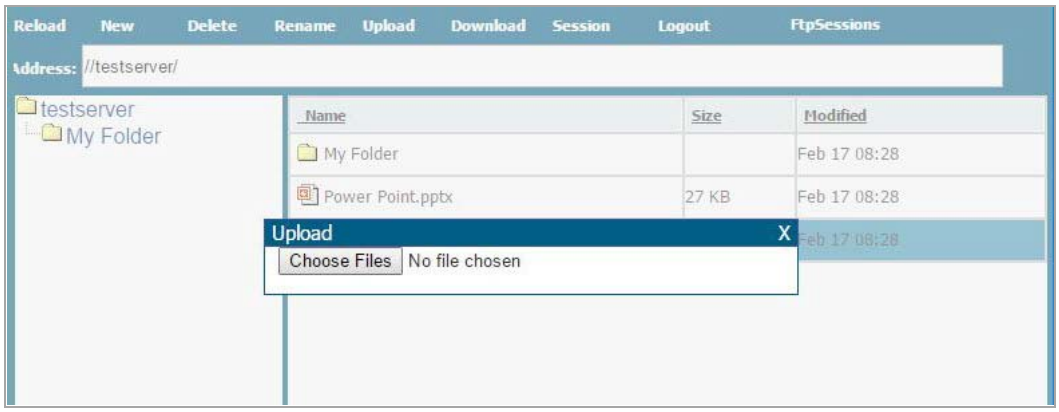


6 Use the buttons across the top of the page to complete actions on the FTP site:

- To reload the page, click **Reload**.
- To add a file or folder, click **Add**. You can also drag and drop files onto the page.
- To delete a file or folder, select it and then click **Delete**.
- To rename a file or folder, select it and then click **Rename**. Edit the name and then click the green checkmark.



- To upload a file, click **Upload**. Click **Browse** to locate the file and select it.



- To Download a file, click **Download** and then click the name of the file. If a File Download Security Warning displays, click **Run** to launch the file or click **Save** to save it to your computer.
- To initiate another FTP session, click **Session**.
- To log out of the FTP session, click **Logout**.
- To move between multiple FTP sessions, click **FtpSessions**.

Using Telnet Bookmarks

To use a Telnet bookmark:

1 Click the Telnet bookmark.

Telnet bookmarks can use a port designation for servers not running on the default port.

2 Click **OK** to any warning messages that are displayed.

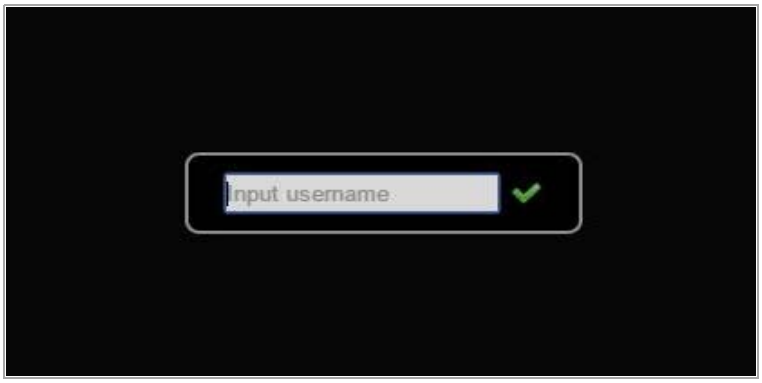
3 If the device you are Telnetting to is configured for authentication, enter your username and password in the custom credentials fields.

Using SSHv2 Bookmarks

SSHv2 bookmarks can use a port designation for servers not running on the default port.

To use an SSHv2 bookmark:

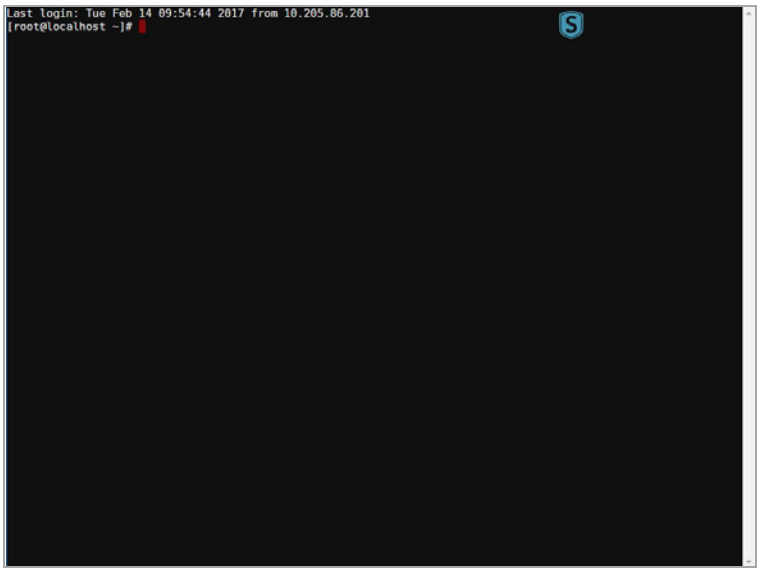
1 Click the SSHv2 bookmark. To **Use custom credentials**, type your user name and password in the **Username** and **Password** field and click **OK**.



2 A hostkey popup displays. Click **Yes** to accept and proceed with the login process.

3 Enter your password and click **OK**.

4 The SSH terminal launches in a new screen.

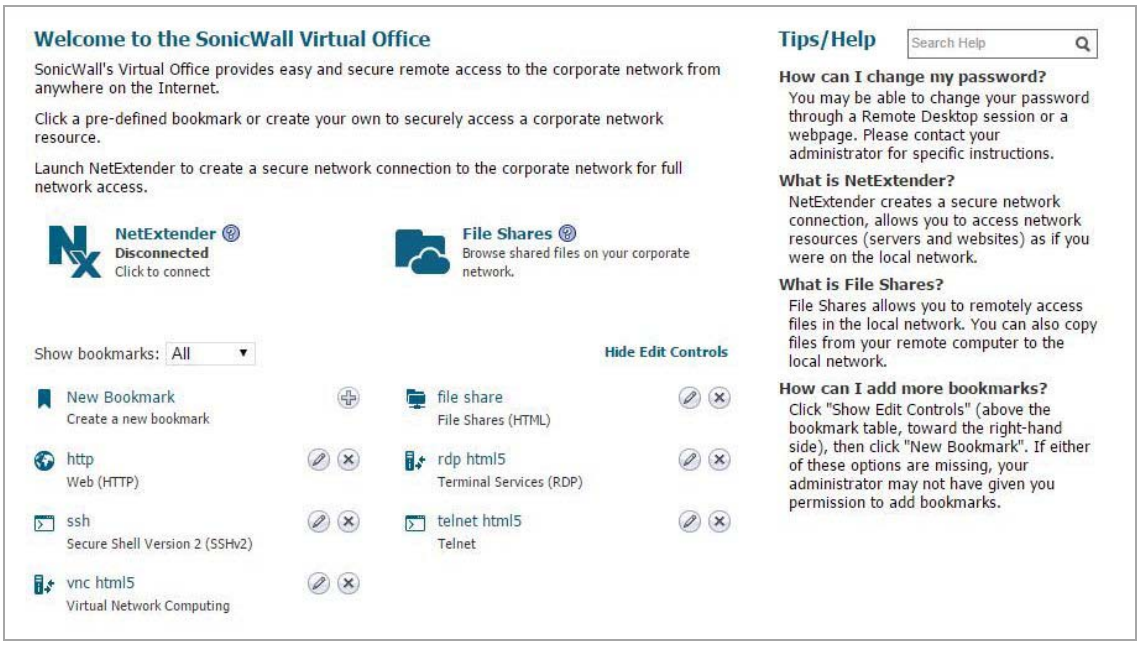


Global Bookmark Single Sign-On Options

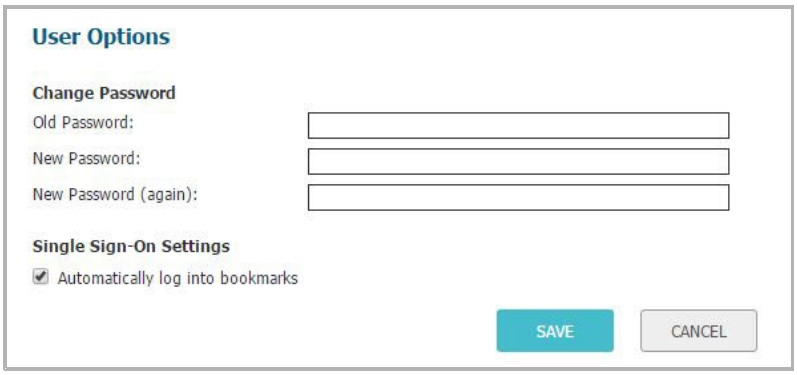
You can configure single sign-on using **Options** on the main Virtual Office page. SSO settings are enabled only if the Administrator has configured user- controlled single sign-on (SSO).

To configure SSO bookmark options:

1 Click **Options** at the top right of the Virtual Office. The **User Options** page displays.



2 Under **Single Sign-On Settings**, select **Use SSL VPN account credentials to log in to bookmarks** to enable SSO for bookmarks. Leave the box cleared if you do not want to use SSO for bookmarks.



3 Click **Save** to save your changes.

Fileshares are used the configured domain name of which the user is a member to supply to the backend server. HTTP, HTTPS, FTP, RDP supplies the username and password that were used to login. If the server is expecting a domain-prefixed username, SSO fails. In some cases, a default domain can be specified at the server to allow SSO to succeed.

Per-Bookmark Single Sign-On Options

Secure Mobile Access supports per-bookmark single sign-on for the following bookmark services:

- Terminal Services (RDP)
- Web (HTTP)
- Secure Web (HTTPS)
- File Shares (CIFS)
- File Transfer Protocol (FTP)

Per-Bookmark SSO allows users to enable or disable SSO for individual bookmarks. This flexibility in specifying login credentials is useful in the following cases:

- Users who use multiple accounts to access a variety of resources.
- Users who use two-factor authentication to log in to the Secure Mobile Access Virtual Office, but use a static password to access other resources.
- Users who need to access servers that require a domain prefix.

To configure per-bookmark SSO:

1 Before enabling SSO on an individual bookmark, you must first enable SSO globally as described in Global Bookmark Single Sign-On Options on page 145.

2 On the Virtual Office page, click **New Bookmark**.

3 Select one of the service types that supports per-bookmark SSO: **Terminal Services (RDP)**, **Secure Web (HTTPS)**, **File Shares (CIFS)**, or **File Transfer Protocol (FTP)**.

4 To disable SSO for the bookmark, clear the **Automatically log in** check box.

5 To use SSO for the bookmark, select the **Automatically log in** check box and then select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow login to the bookmark using the local user credentials configured on the SMA/SRA appliance.
- **Use custom credentials** – allow login to the bookmark using the credentials you enter here; when selected, this option displays **Username**, **Password**, and **Domain** fields. Enter the custom credentials into the **Username**, **Password**, and **Domain** fields that are displayed.

You can enter the custom credentials as text or use dynamic variables such as those shown in the SSO Credentials: Dynamic Variables table:

SSO Credentials: Dynamic Variables

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%
Password	%PASSWORD%	%PASSWORD% or leave the field blank

6 For Web (HTTP) and Secure Web (HTTPS) bookmarks, select the **Forms-based Authentication** check box to use this method for SSO, and then fill in the following fields that are exposed:

- Configure the **User Form Field** to be the same as the ‘name’ or ‘id’ attribute of the HTML element representing User Name in the Login form, for example:

  <input type=text name=’userid’>

- Configure the **Password Form Field** to be the same as the ‘name’ or ‘id’ attribute of the HTML element representing Password in the Login form, for example:

  <input type=password name=’PASSWORD’ id=’PASSWORD’ maxlength=128>

7 Click **OK**.

8 Enter the **User name** and **password** for the service.

Part 3

Appendix

- Warranty and License Agreements

A

Warranty and License Agreements

This appendix contains the following sections:

- GNU General Public License (GPL) Source Code on page 149
- Limited Hardware Warranty on page 149
- End User License Agreement on page 150

GNU General Public License (GPL) Source Code

SonicWall provides a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, send your written request, along with a certified check or money order in the amount of US $25.00 payable to “SonicWall, Inc.” to:

General Public License Source Code Request
SonicWall, Inc. Attn: Jennifer Anderson

5455 Great America Parkway
Santa Clara, CA 95054

Limited Hardware Warranty

All SonicWall appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. Visit the Warranty Information page for details on your product’s warranty:
https://support.sonicwall.com/essentials/support-offerings

SonicWall, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWall), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWall and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWall's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWall's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWall's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWall.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR

JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWall or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

End User License 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.

B

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.