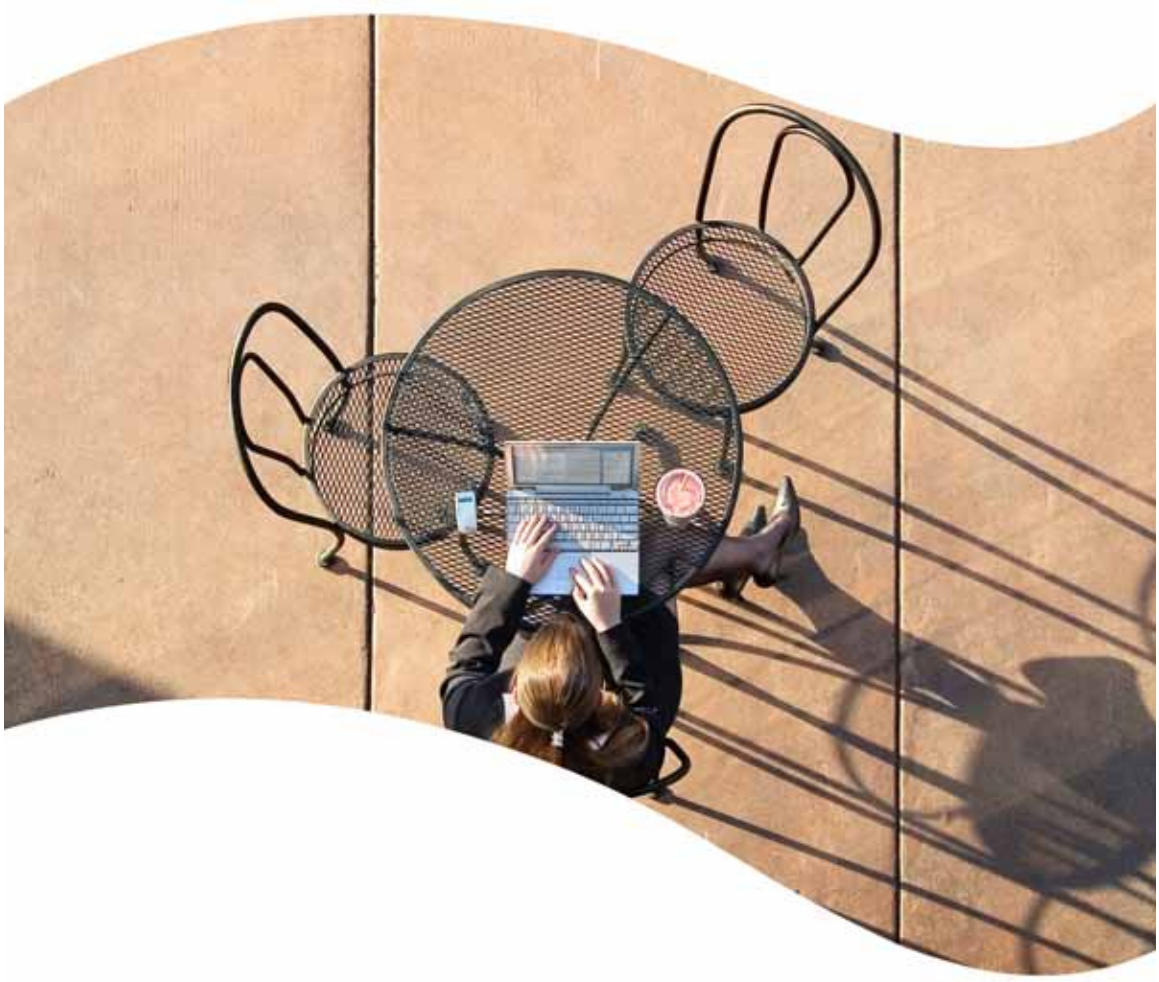
SonicWALL Secure Remote Access Appliances

SonicWALL SSL VPN 4.0 Administrator's Guide

SONICWALL®



SonicWALL SSL VPN 4.0 Administrator's Guide

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452

Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Copyright Notice

Trademarks

SonicWALL GPL Source Code

GNU General Public License (GPL)

SonicWALL will provide 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
2001 Logic Drive
San Jose, CA 95124-3452

Limited Warranty

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.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at *<http://www.sonicwall.com/us/support.html>*. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below. See *<http://www.sonicwall.com/us/support/contact.html>* for the latest technical support telephone numbers.

North America Telephone Support

U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Australia - + 1800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39.02.7541.9803

Japan - + 81(0)3.3457.8971

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41.1.308.3.977

UK - +44(0)1344.668.484

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408) 745-9300

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

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

About This Guide

The *SonicWALL SSL VPN Administrator's Guide* provides network administrators with a high-level overview of SonicWALL SSL VPN technology, including activation, configuration, and administration of the SonicWALL SSL VPN management interface and the SonicWALL SSL-VPN appliance.

Note Always check <http://www.sonicwall.com/support/documentation.html> for the latest version of this guide as well as other SonicWALL products and services documentation.

Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights dialog box, window, and screen names. Also highlights buttons and tabs. 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, emphasis on certain words in a sentence, or the first instance of a significant term or concept.
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, **System > Status** means select the **Status** page under the **System** menu.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

Tip Useful information about security features and configurations on your SonicWALL.

Note Important information on a feature that requires callout for special attention.

Timesaver Useful tips about features that may save you time

Indicates a feature that is supported only on the SSL-VPN 2000 and 4000 platforms.

Indicates a client feature that is only supported on the Microsoft Windows platform.

Indicates a client feature that is supported on Microsoft Windows, Apple MacOS, and Linux

Organization of This Guide

The *SonicWALL SSL VPN Administrator's Guide* is organized in chapters that follow the SonicWALL SSL VPN Web-based management interface structure.

This section contains a description of the following chapters and appendices:

SSL VPN Overview

"SSL VPN Overview" on page 7 provides an introduction to SSL VPN technology and an overview of the SonicWALL SSL-VPN appliance and Web-based management interface features. The SSL VPN Overview chapter includes SSL VPN concepts, a Web-based management interface overview, and deployment guidelines.

System Configuration

"System Configuration" on page 59 provides instructions for configuring SonicWALL SSL VPN options under **System** in the navigation bar of the management interface, including:

- Registering the SonicWALL appliance
- Setting the date and time
- Working with configuration files
- Managing firmware versions and preferences
- General appliance administration
- Certificate management
- Viewing SSL VPN monitoring reports
- Using diagnostic tools

Network Configuration

"Network Configuration" on page 91 provides instructions for configuring SonicWALL SSL VPN options under **Network** in the navigation bar of the management interface, including:

- Configuring network interfaces
- Configuring DNS settings
- Setting network routes and static routes
- Configuring hostname and IP address information for internal name resolution
- Creating reusable network objects representing network resources like FTP, HTTP, RDP, SSH and File Shares

Portals Configuration

"Portals Configuration" on page 105 provides instructions for configuring SonicWALL SSL VPN options under **Portals** in the navigation bar of the management interface, including portals, domains (including RADIUS, NT, LDAP and Active Directory authentication), and custom logos.

NetExtender Configuration

"NetExtender Configuration" on page 159 provides instructions for configuring SonicWALL SSL VPN options under **NetExtender** in the navigation bar of the management interface, including NetExtender status, setting NetExtender address range, and configuring NetExtender routes.

Virtual Assist Configuration

"Virtual Assist Configuration" on page 169 provides instructions for configuring SonicWALL SSL VPN options under **Virtual Assist** in the navigation bar of the management interface, including Virtual Assist status, settings and licensing.

Web Application Firewall Configuration

"Web Application Firewall Configuration" on page 179 provides instructions for configuring SonicWALL SSL VPN options under Web Application Firewall in the navigation bar of the management interface, including Web Application Firewall status, settings, signatures, log, and licensing.

Users Configuration

"Users Configuration" on page 201 provides instructions for configuring SonicWALL SSL VPN options under **Users** in the navigation bar of the management interface, including:

- Access policy hierarchy overview
- Configuring local users and local user policies
- Configuring user groups and user group policies
- Global configuration

Log Configuration

"Log Configuration" on page 253 provides instructions for configuring SonicWALL SSL VPN options under **Log** in the navigation bar of the management interface, including viewing and configuring logs and creating alert categories.

Virtual Office Configuration

"Virtual Office Configuration" on page 265 provides a brief introduction to the Virtual Office, the user portal feature of SonicWALL SSL VPN. The administrator can access the Virtual Office user portal using **Virtual Office** in the navigation bar of the SonicWALL SSL VPN Web-based management interface. Users access the Virtual Office using a Web browser. The *SonicWALL SSL VPN User's Guide* provides detailed information about the Virtual Office.

Appendix A: Accessing Online Help

"Online Help" on page 269 provides a description of the help available from the **Online Help** button in the upper right corner of the management interface. This appendix also includes an overview of the context-sensitive help found on most pages of the SonicWALL SSL VPN management interface.

Appendix B: Configuring SonicWALL SSL VPN with a Third-Party Gateway

"Configuring SonicWALL SSL VPN with a Third-Party Gateway" on page 271 provides configuration instructions for configuring the SonicWALL SSL-VPN appliance to work with third-party gateways, including:

- Cisco PIX
- Linksys WRT54GS
- WatchGuard Firebox X Edge
- NetGear FVS318
- Netgear Wireless Router MR814
- Check Point AIR 55
- Microsoft ISA Server 2000

Appendix C: Use Cases

"Use Cases" on page 291 provides use cases for importing CA certificates and for configuring group-based access policies for multiple Active Directory groups needing access to Outlook Web Access and SSH.

Appendix D: NetExtender Troubleshooting

"NetExtender Troubleshooting" on page 309 provides troubleshooting support for the SonicWALL SSL VPN NetExtender feature.

Appendix E: FAQ

"FAQs" on page 313 provides a list of frequently asked questions about the SonicWALL SSL VPN Web-based management interface and SonicWALL SSL-VPN appliance.

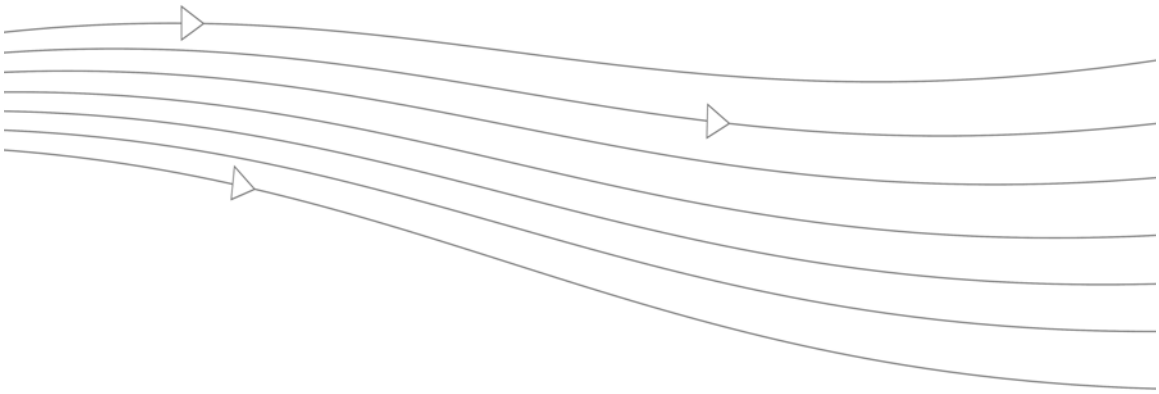
Appendix F: Glossary

"Glossary" on page 337 provides a glossary of technical terms used in the *SonicWALL SSL VPN Administrator's Guide*.

Appendix G: SMS Email Formats

"SMS Email Formats" on page 339 provides a list of SMS email formats for selected worldwide cellular carriers.

Table of Contents



Chapter 1: SSL VPN Overview

This chapter provides an overview of the SonicWALL SSL VPN technology, concepts, basic navigational elements and standard deployment guidelines. This chapter includes the following sections:

Overview of SonicWALL SSL VPN

The SonicWALL SSL-VPN appliance provides organizations with a simple, secure and clientless method of access to applications and network resources specifically for remote and mobile employees. Organizations can use SonicWALL SSL VPN connections without the need to have a pre-configured, large-installation host. Users can easily and securely access email files, intranet sites, applications, and other resources on the corporate Local Area Network (LAN) from any location by accessing a standard Web browser.

Organizations use Virtual Private Networks (VPNs) to establish secure, end-to-end private network connections over a public networking infrastructure, allowing them to reduce their communications expenses and to provide private, secure connections between a user and a site in the organization. By offering Secure Socket Layer (SSL) VPN, without the expense of special feature licensing, the SonicWALL SSL-VPN appliance provides customers with cost-effective alternatives to deploying parallel remote-access infrastructures. This section contains the following subsections:

- "SSL for Virtual Private Networking (VPN)" section on page 8
- "SSL VPN Software Components" section on page 9
- "SSL-VPN Hardware Components" section on page 9

SSL for Virtual Private Networking (VPN)

A Secure Socket Layer-based Virtual Private Network (SSL VPN) allows applications and private network resources to be accessed remotely through a secure connection. Using SSL VPN, mobile workers, business partners, and customers can access files or applications on a company's intranet or within a private local area network.

Although SSL VPN protocols are described as clientless, the typical SSL VPN portal combines Web, Java, and ActiveX components that are downloaded from the SSL VPN portal transparently, allowing users to connect to a remote network without needing to manually install and configure a VPN client application. In addition, SSL VPN enables users to connect from a variety of devices, including Windows, Macintosh, and Linux PCs. ActiveX components are only supported on Windows platforms.

For administrators, the SonicWALL SSL VPN Web-based management interface provides an end-to-end SSL VPN solution. This interface can configure SSL VPN users, access policies, authentication methods, user bookmarks for network resources, and system settings.

For clients, Web-based SonicWALL SSL VPN customizable user portals enable users to access, update, upload, and download files and use remote applications installed on desktop machines or hosted on an application server. The platform also supports secure Web-based FTP access, network neighborhood-like interface for file sharing, Secure Shell versions 1 and 2 (SSHv1) and (SSHv2), Telnet emulation, VNC (Virtual Network Computing) and RDP (Remote Desktop Protocol) support, Citrix Web access, bookmarks for offloaded portals (external Web sites), and Web and HTTPS proxy forwarding.

The SonicWALL SSL VPN network extension client, NetExtender, is available through the SSL VPN Web portal via an ActiveX control on Windows or using Java on MacOS or Linux systems. It is also available through stand-alone applications for Windows, Linux, and MacOS platforms. The NetExtender standalone applications are automatically installed on a client system the first time the user clicks the NetExtender link in the Virtual Office portal. SonicWALL SSL VPN NetExtender enables end users to connect to the remote network without needing to install and configure complex software, providing a secure means to access any type of data on the remote network. When used with a SonicWALL SSL-VPN 2000 or higher model, NetExtender supports IPv6 client connections from Windows systems running Vista or newer, and from Linux clients.

Note The SSHv2 applet requires SUN JRE 1.6.0_10 or higher and can only connect to a server that supports SSHv2. The RDP Java applet requires SUN JRE 1.6.0_10 or higher. Telnet, SSHv1 and VNC applets support MS JVM in Internet Explorer, and run on other browsers with SUN JRE 1.6.0_10 or higher.

SSL VPN Software Components

SonicWALL SSL VPN provides clientless identity-based secure remote access to the protected internal network. Using the Virtual Office environment, SonicWALL SSL VPN can provide users with secure remote access to your entire private network, or to individual components such as File Shares, Web servers, FTP servers, remote desktops, or even individual applications hosted on Microsoft Terminal Servers.

SSL-VPN Hardware Components

See the following section for descriptions of the hardware components on SonicWALL SSL-VPN appliances:

- "SSL-VPN 2000 and 4000 Front and Back Panels Overview" on page 9

SSL-VPN 2000 and 4000 Front and Back Panels Overview

Figure 1 SonicWALL SSL-VPN 2000 Front and Back Panels

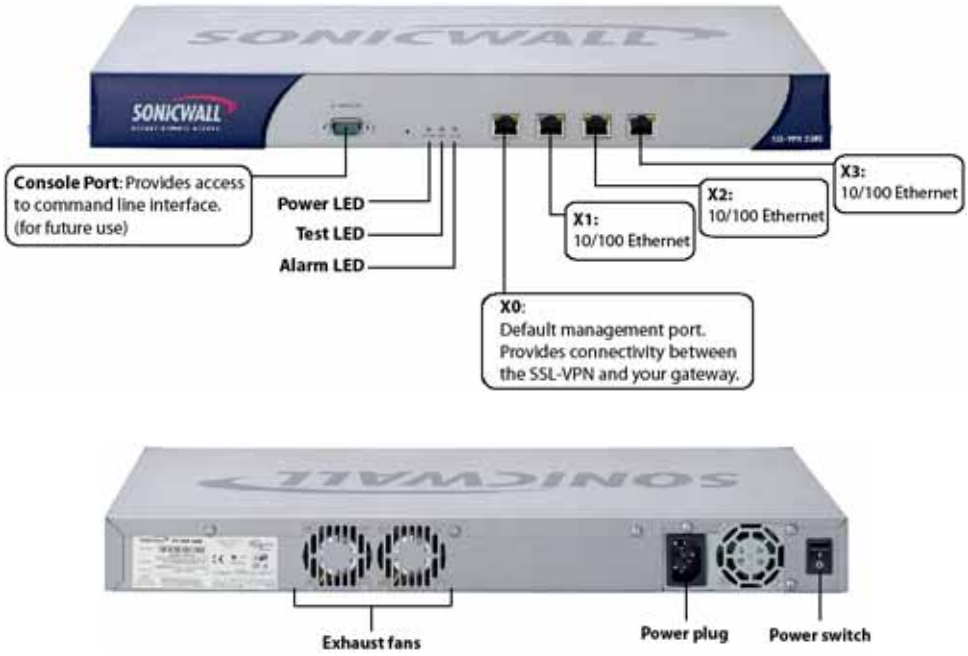


Figure 2 SonicWALL SSL-VPN 4000 Front and Back Panels

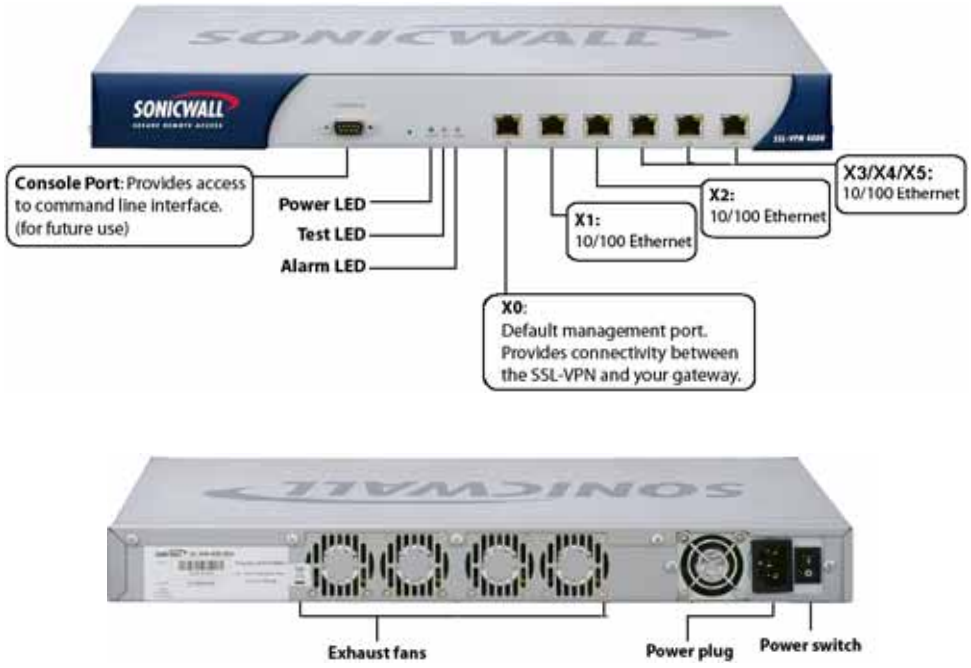


Table 1 SonicWALL SSL-VPN 2000/4000 Front Panel Features

Front Panel Feature	Description
Console Port	Provides access to command-line interface.
Power LED	Indicates the SonicWALL SSL-VPN appliance is powered on.
Test LED	Indicates the SonicWALL SSL-VPN is in test mode.
Alarm LED	Indicates a critical error or failure.
X0	Default management port. Provides connectivity between the SonicWALL SSL-VPN and your gateway.
X1	Provides access to the X1 interface and to SSL VPN resources.
X2	Provides access to the X2 interface and to SSL VPN resources.
X3	Provides access to the X3 interface and to SSL VPN resources.
X4 (4000 only)	Provides access to the X4 interface and to SSL VPN resources.
X5 (4000 only)	Provides access to the X5 interface and to SSL VPN resources.

Table 2 SonicWALL SSL-VPN 2000/4000 Back Panel Features

Back Panel Feature	Description
Exhaust fans	Provides optimal cooling for the SonicWALL SSL-VPN appliance.
Power plug	Provides power connection using supplied power cord.
Power switch	Powers the SonicWALL SSL-VPN appliance on and off.

Concepts for SonicWALL SSL VPN

This section provides an overview of the following key concepts, with which the administrator should be familiar when using the SonicWALL SSL-VPN appliance and Web-based management interface:

Encryption Overview

Encryption enables users to encode data, making it secure from unauthorized viewers. Encryption provides a private and secure method of communication over the Internet.

A special type of encryption known as Public Key Encryption (PKE) comprises a public and a private key for encrypting and decrypting data. With public key encryption, an entity, such as a secure Web site, generates a public and a private key. A secure Web server sends a public key to a user who accesses the Web site. The public key allows the user's Web browser to decrypt data that had been encrypted with the private key. The user's Web browser can also transparently encrypt data using the public key and this data can only be decrypted by the secure Web server's private key.

Public key encryption allows the user to confirm the identity of the Web site through an SSL certificate. After a user contacts the SSL-VPN appliance, the appliance sends the user its own encryption information, including an SSL certificate with a public encryption key.

SSL Handshake Procedure

The following procedure is an example of the standard steps required to establish an SSL session between a user and an SSL VPN gateway using the SonicWALL SSL VPN Web-based management interface:

Step 1 When a user attempts to connect to the SonicWALL SSL-VPN appliance, the user's Web browser sends information about the types of encryption supported by the browser to the appliance.

Step 2 The appliance sends the user its own encryption information, including an SSL certificate with a public encryption key.

Step 3 The Web browser validates the SSL certificate with the Certificate Authority identified by the SSL certificate.

Step 4 The Web browser generates a pre-master encryption key, encrypts the pre-master key using the public key included with the SSL certificate and sends the encrypted pre-master key to the SSL VPN gateway.

Step 5 The SSL VPN gateway uses the pre-master key to create a master key and sends the new master key to the user's Web browser.

Step 6 The browser and the SSL VPN gateway use the master key and the agreed upon encryption algorithm to establish an SSL connection. From this point on, the user and the SSL VPN gateway will encrypt and decrypt data using the same encryption key. This is called symmetric encryption.

Step 7 Once the SSL connection is established, the SSL VPN gateway will encrypt and send the Web browser the SSL VPN gateway login page.

Step 8 The user submits his user name, password, and domain name.

Step 9 If the user's domain name requires authentication through a RADIUS, LDAP, NT Domain, or Active Directory Server, the SSL VPN gateway forwards the user's information to the appropriate server for authentication.

Step 10 Once authenticated, the user can access the SSL VPN portal.

IPv6 Support Overview

Internet Protocol version 6 (IPv6) is a replacement for IPv4 that is becoming more frequently used on networked devices. IPv6 is a suite of protocols and standards developed by the Internet Engineering Task Force (IETF) that provides a larger address space than IPv4, additional functionality and security, and resolves IPv4 design issues. You can use IPv6 without affecting IPv4 communications.

Supported on SonicWALL SSL-VPN models 2000 and higher, IPv6 supports stateful address configuration, which is used with a DHCPv6 server, and stateless address configuration, where hosts on a link automatically configure themselves with IPv6 addresses for the link, called *link-local* addresses.

In IPv6, source and destination addresses are 128 bits (16 bytes) in length. For reference, the 32-bit IPv4 address is represented in dotted-decimal format, divided by periods along 8-bit boundaries. The 128-bit IPv6 address is divided by colons along 16-bit boundaries, where each 16-bit block is represented as a 4-digit hexadecimal number. This is called colon-hexadecimal.

The IPv6 address, 2008:0AB1:0000:1E2A:0123:0045:EE37:C9B4 can be simplified by removing the leading zeros within each 16-bit block, as long as each block has at least one digit. When suppressing leading zeros, the address representation becomes: 2008:AB1:0:1E2A:123:45:EE37:C9B4

When addresses contain contiguous sequences of 16-bit blocks set to zeros, the sequence can be compressed to **::**, a double-colon. For example, the link-local address of 2008:0:0:0:B67:89:ABCD:1234 can be compressed to 2008::B67:89:ABCD:1234. The multicast address 2008:0:0:0:0:0:0:2 can be compressed to 2008::2.

The IPv6 prefix is the part of the address that indicates the bits of the subnet prefix. Prefixes for IPv6 subnets, routes, and address ranges are written as address/prefix-length, or CIDR notation. For example, 2008:AA::/48 and 2007:BB:0:89AB::/64 are IPv6 address prefixes.

SonicOS SSL VPN supports IPv6 in the following areas:

Services

- **FTP Bookmark** – Define a FTP bookmark using an IPv6 address.
- **Telnet Bookmark** – Define a Telnet bookmark using an IPv6 address.
- **SSHv1 / SSHv2 Bookmark** – Define an SSHv1 or SSHv2 bookmark using an IPv6 address.
- **Reverse proxy for HTTP/HTTPS Bookmark** – Define an HTTP or HTTPS bookmark using an IPv6 address.
- **Citrix Bookmark** – Define a Citrix bookmark using an IPv6 address.
- **RDP Bookmark -** Define an RDP bookmark using an IPv6 address.
- **VNC Bookmark -** Define a VNC bookmark using an IPv6 address.

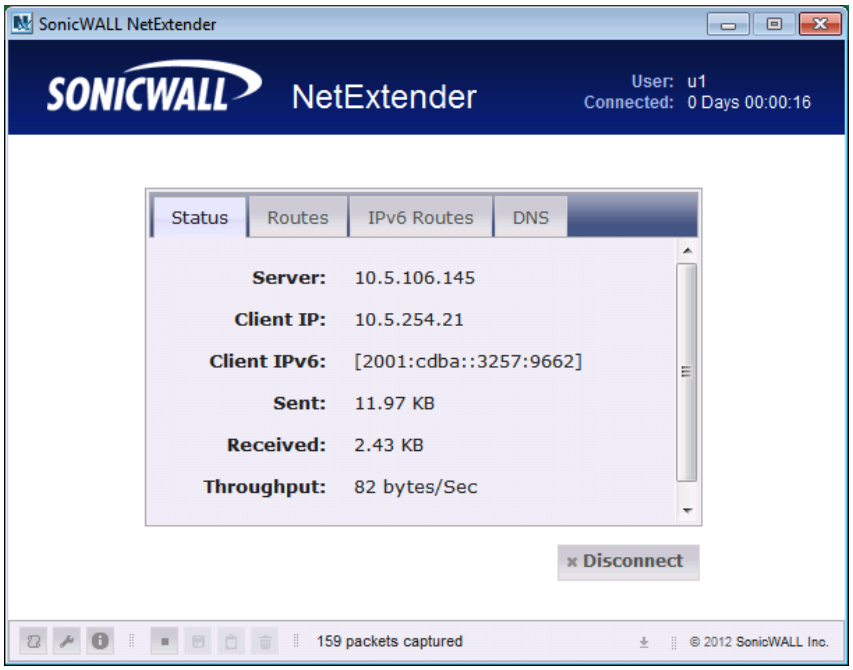
Note IPv6 is not supported for File Shares.

Settings

- **Interface Settings** – Define an IPv6 address for the interface. The **link-local** address is displayed in a tooltip on Interfaces page.
- **Route Settings** – Define a static route with IPv6 destination network and gateway.
- **Network Object** – Define the network object using IPv6. An IPv6 address and IPv6 network can be attached to this network object.

NetExtender

When a client connects to NetExtender, it can get an IPv6 address from the SSL-VPN appliance if the client machine supports IPv6 and an IPv6 address pool is configured on the SSL-VPN. NetExtender supports IPv6 client connections from Windows systems running Vista or newer, and from Linux clients.



Virtual Assist

Users and Technicians can request and provide support when using IPv6 addresses.

Rules

- **Policy rule** – User or Group Policies. Three IPv6 options in the **Apply Policy To** drop-down list:
  - **IPv6 Address**
  - **IPv6 Address Range**
  - **All IPv6 Address**
- **Login rule** – Use IPv6 for address fields:
  - Define **Login From Defined Addresses** using IPv6
  - Two IPv6 options in the **Source Address** drop-down list: **IPv6 Address** / **IPv6 Network**

Virtual Hosts

An administrator can assign an IPv6 address to a virtual host, and can use this address to access the virtual host.

Application Offloading

An administrator can assign an IPv6 address to an application server used for application offloading, and can use this address to access the server.

Browser Requirements for the SSL VPN Administrator

The following Web browsers are supported for the SonicWALL SSL VPN Web-based management interface and the user portal, **Virtual Office**. Java is only required for various aspects of the SSL VPN Virtual Office, not the management interface.

- Internet Explorer 8.0 or newer
- Mozilla Firefox 11.0 or newer
- Google Chrome 18.0 or newer

The following table provides specific browser requirements.

SSL VPN Management Interface Minimum Browser/Version Requirements	Windows XP	Windows Vista	Windows 7	Linux	MacOS X
Browser	8	9	9		5
	11	11	11	11	11
	18	18	18	18	18

To configure SonicWALL SSL-VPN appliance using the Web-based management interface, an administrator must use a Web browser with Java, JavaScript, ActiveX, cookies, popups, and SSLv3 or TLS 1.0 enabled.

Browser Requirements for the SSL VPN End User

The following is a list of Web browser and operating system support for various SSL VPN protocols including NetExtender and various Application Proxy elements. Requirements are shown for Windows XP, Windows 7, Windows Vista, Linux, and MacOS.

Portals Overview

The SonicWALL SSL-VPN appliance provides a mechanism called Virtual Office, which is a Web-based *portal* interface that provides clients with easy access to internal resources in your organization. Components such as NetExtender, Virtual Assist, and bookmarks to file shares and other network resources are presented to users through the Virtual Office portal. For organizations with multiple user types, the SSL-VPN allows for multiple customized portals, each with its own set of shared resource bookmarks. Portals also allow for individual domain and security certificates on a per-portal basis. The components in a portal are customized when adding a portal.

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. File shares can be configured to allow restricted server path access.

Custom Portals

SonicWALL SSL VPN enables you to configure multiple portals, each with its own title, banner, login message, logo and set of available resources. Each portal also enables you to set individual Virtual Hosts/Domain Names (on SonicWALL SSL-VPN models 2000 and higher) to create a unique default portal URL. When a user logs into a portal, he or she sees a set of pre-configured links and bookmarks that are specific to that portal. You can configure whether or not NetExtender is displayed on a Virtual Office portal, and if you want

NetExtender to automatically launch when users log in to the portal. The administrator configures which elements each portal displays through the **Portal Settings** dialog box. For information on configuring portals, refer to the "Portals > Portals" section on page 106.

Domains Overview

A domain in the SonicWALL SSL VPN environment is a mechanism that enables authentication of users attempting to access the network being serviced by the SSL-VPN appliance. Domain types include the SSL VPN's internal LocalDomain, and the external platforms Microsoft Active Directory, NT Authentication, LDAP, and RADIUS. Often, only one domain will suffice to provide authentication to your organization, although a larger organization may require distributed domains to handle multiple nodes or collections of users attempting to access applications through the portal. For information about configuring domains, refer to the "Portals > Domains" section on page 122.

NetExtender Overview

This section provides an overview to the NetExtender feature. This section contains the following subsections:

For information on using NetExtender, refer to the "NetExtender > Status" section on page 160 or refer to the *SonicWALL SSL VPN User's Guide*.

What is NetExtender?

SonicWALL NetExtender is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

Benefits

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPSec VPN client, but NetExtender does not require any manual client installation. Instead, the NetExtender Windows client is automatically installed on a remote user's PC by an ActiveX control when using the Internet Explorer browser, or with the XPCOM plugin when using Firefox. On Linux or MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal.

The NetExtender Windows client also has a custom-dialer that allows it to be launched from the Windows **Network Connections** menu. This custom-dialer allows NetExtender to be connected before the Windows domain login. The NetExtender Windows client also supports a single active connection, and displays real-time throughput and data compression ratios in the client.

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.

NetExtender Concepts

The following sections describe advanced NetExtender concepts:

Stand-Alone Client

SonicWALL SSL VPN provides a stand-alone NetExtender application. NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user's PC or Mac. The installer creates a profile based on the user's login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer will first uninstall the old NetExtender and install the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in /usr/share/NetExtender. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Multiple Ranges and Routes

Multiple range and route support for NetExtender on SonicWALL SSL-VPN models 2000 and higher enables network administrators to easily segment groups and users without the need to configure firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it.

For networks that do not require segmentation, client addresses and routes can be configured globally as in the SSL VPN 1.0 version of NetExtender. The following sections describe the new multiple range and route enhancements:

IP Address User Segmentation

Administrators can configure separate NetExtender IP address ranges for users and groups. These settings are configured on the **Users > Local Users** and **Users > Local Groups** pages, using the **NetExtender** tab in the **Edit User** and **Edit Group** windows.

When configuring multiple user and group NetExtender IP address ranges, it is important to know how the SonicWALL SSL-VPN appliance assigns IP addresses. When assigning an IP address to a NetExtender client, the SonicWALL SSL-VPN appliance uses the following hierarchy of ranges:

1. An IP address from the range defined in the user's local profile.
2. An IP address from the range defined in the group profile to which the user belongs.
3. An IP address from the global NetExtender range.

To reserve a single IP address for an individual user, the administrator can enter the same IP address in both the **Client Address Range Begin** and **Client Address Range End** fields on the **NetExtender** tab of the **Edit Group** window.

Client Routes

NetExtender client routes are used to allow and deny access to various network resources. Client routes can also be configured at the user and group level. NetExtender client routes are also configured on the **Edit User** and **Edit Group** windows. The segmentation of client routes is fully customizable, allowing the administrator to specify any possible permutation of user, group, and global routes (such as only group routes, only user routes, group and global routes, user, group, and global routes, etc.). This segmentation is controlled by the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** checkboxes.

NetExtender with External Authentication Methods

Networks that use an external authentication server will not configure local usernames on the SonicWALL SSL-VPN appliance. In such cases, when a user is successfully authenticated, a local user account is created if the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** settings are enabled.

Point to Point Server IP Address

In SonicWALL SSL VPN, the PPP server IP address is 192.0.2.1 for all connecting clients. This IP address is transparent to both the remote users connecting to the internal network and to the internal network hosts communicating with remote NetExtender clients. Because the PPP server IP address is independent from the NetExtender address pool, all IP addresses in the global NetExtender address pool will be used for NetExtender clients.

Connection Scripts

SonicWALL SSL VPN 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. NetExtender Connection Scripts can support any valid batch file commands.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

Tunnel All mode can be configured at the global, group, and user levels.

Proxy Configuration

SonicWALL SSL VPN 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. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

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)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP 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 and bypass the proxy server. If required, you can 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, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the SSL VPN server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

Network Resources Overview

Network Resources are the granular components of a trusted network that can be accessed using SonicWALL SSL VPN. Network Resources can be pre-defined by the administrator and assigned to users or groups as bookmarks, or users can define and bookmark their own Network Resources.

The following sections describe types of network resources supported by SonicWALL SSL VPN:

HTTP (Web) and Secure HTTPS (Web)

The SonicWALL SSL-VPN appliance provides proxy access to an HTTP or HTTPS server on the internal network, Internet, or any other network segment that can be reached by the appliance. The remote user communicates with the SonicWALL SSL-VPN appliance using HTTPS and requests a URL. The URL is then retrieved over HTTP by the SonicWALL SSL-VPN. The URL is transformed as needed, and returned encrypted to the remote user.

The SSL VPN administrator can configure Web (HTTP) or Secure Web (HTTPS) bookmarks to allow user access to Web-based resources and applications such as Microsoft OWA Premium or Domino Web Access 7 with HTTP(S) reverse proxy support. Reverse-proxy bookmarks also support the HTTP 1.1 protocol and connection persistence.

HTTPS bookmarks on the SSL-VPN 2000 and SSL-VPN 4000 appliances support keys of up to 2048 bits. The SSL-VPN 200 appliance supports keys of up to 1024 bits.

HTTP(S) caching is supported on the SSL-VPN appliance for use when it is acting as a proxy Web server deployed between a remote user and a local Web server. The proxy is allowed to cache HTTP(S) content on the SSL-VPN appliance which the internal Web server deems cacheable based on the HTTP(S) protocol specifications. For subsequent requests, the cached content is returned only after ensuring that the user is authenticated with the SSL-VPN device and is cleared for access by the access policies. However, SSL VPN 4.0 optimizes traffic to the backend webserver by using TCP connection multiplexing, where a single TCP connection is used for multiple user sessions to the same web server. Caching is predominantly used for static Web content like JavaScript files, style sheets, and images. The proxy can parse HTML/JavaScript/CSS documents of indefinite length. The administrator can enable or disable caching, flush cached content and set the maximum size for the cache.

Content received by the SonicWALL SSL-VPN appliance from the local Web server is compressed using *gzip* before sending it over the Internet to the remote client. Compressing content sent from the SSL-VPN saves bandwidth and results in higher throughput.

Furthermore, only compressed content is cached, saving nearly 40-50% of the required memory. Note that gzip compression is not available on the local (clear text side) of the SSL-VPN appliance, or for HTTPS requests from the remote client.

Telnet (Java)

A Java-based Telnet client delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible Telnet server and SonicWALL SSL VPN will make a connection to the server. Communication between the user over SSL and the server is proxied using native Telnet. The Telnet applet supports MS JVM (Microsoft Java Virtual Machine) in Internet Explorer, and requires Sun Java Runtime Environment (JRE) 1.1 or higher for other browsers.

SSHv1 and SSHv2 (Java)

Java-based SSH clients delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible SSH server and SonicWALL SSL VPN will make a connection to the server. Communication between the user over SSL and the server is proxied using natively encrypted SSH. The SSHv1 applet supports MS JVM in Internet Explorer, and requires SUN JRE 1.1 for other browsers. SSHv2 provides stronger encryption and has other advanced features, and can only connect to a server that supports SSHv2. SSHv2 support sets the terminal type to VT100. SSHv2 requires JRE 1.6.0_10 or higher, available from http://java.sun.com.

FTP (Web)

Proxy access to an FTP server on the internal network, the Internet, or any other network segment that can be reached by the SSL-VPN appliance. The remote user communicates with the SSL-VPN appliance by HTTPS and requests a URL that is retrieved over HTTP by SonicWALL SSL VPN, transformed as needed, and returned encrypted to the remote user. FTP supports 25 character sets, including four Japanese sets, two Chinese sets, and two Korean sets. The client browser and operating system must support the desired character set, and language packs may be required.

File Shares (CIFS)

File Shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or the older 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. File shares can be configured to allow restricted server path access.

Remote Desktop Protocols and Virtual Network Computing

RDP Java and VNC are supported on Windows, Linux, and Mac operating systems, while RDP ActiveX is supported only on Windows. Most Microsoft workstations and servers have RDP server capabilities that can be enabled for remote access, and there are a number of freely available VNC servers that can be downloaded and installed on most operating systems. The RDP and VNC clients are automatically delivered to authorized remote users through their Web browser in the following formats:

- **RDP Java** – RDP Java is a Microsoft Remote Desktop Protocol that has the advantage of broad platform compatibility because it is provided in a Java client. The RDP Java client runs on Windows, Linux, and Mac computers, and supports full-screen mode. On Windows clients, SonicWALL SSL VPN supports many advanced options. On Mac OS X 10.5 or above, RDP Java supports the Mac native RDC client.
- **RDP ActiveX** - RDP ActiveX is also a Microsoft Remote Desktop Protocol. The RDP ActiveX client only runs on Windows, and is not supported on Mac or Linux computers. Four advanced options are supported by SonicWALL SSL VPN for RDP ActiveX.
- **VNC (Java)** - VNC was originally developed by AT&T, but is today widely available as open source software. Any one of the many variants of VNC servers available can be installed on most any workstation or server for remote access. The VNC client to connect to those servers is delivered to remote users through the Web browser as a Java client.

RDP 6 Support

The SonicWALL SSL-VPN appliance supports connections with RDP 6 clients, and supports the RDP 5 feature set plus four RDP 6 features.

The SonicWALL SSL-VPN appliance supports connections with RDP 6.1 clients. RDC 6.1 is included with the following operating systems:

- Windows Server 2008
- Windows Vista Service Pack 1 (SP1)
- Windows XP Service Pack 3 (SP3)

RDC 6.1 incorporates the following functionality in Windows Server 2008:

- Terminal Services RemoteApp
- Terminal Services EasyPrint driver
- Single Sign-On

For more information, see the “Adding or Editing User Bookmarks” section on page 216.

Application Protocols Using RDP

Applications protocols are RDP sessions that provide access to a specific application rather than to an entire desktop. This allows defined access to an individual application, such as CRM or accounting software. When the application is closed, the session closes. The following RDP formats can be used as applications protocols:

RDP Java – Uses the Java-based RDP client to connect to the terminal server, and to automatically invoke an application at the specified path (for example, **C:\programfiles\microsoft office\office11\winword.exe**)

RDP ActiveX – Uses the ActiveX-based RDP client to connect to the terminal server, and to automatically invoke an application at the specified path (for example, **C:\programfiles\wireshark\wireshark.exe**).

Application Support for SSO, User Policies, Bookmarks

Table 3 provides a list of application-specific support for Single Sign-On (SSO), global/group/user policies, and bookmark Single Sign-On control policies.

Table 3 Application Support

Application	Supports SSO	Global/Group/ User Policies	Bookmark Policies
Terminal Services (RDP - ActiveX)	Yes	Yes	Yes
Terminal Services (RDP - Java)	Yes	Yes	Yes
Virtual Network Computing (VNC)	No	Yes	No
File Transfer Protocol (FTP)	Yes	Yes	Yes
Telnet	No	Yes	No
Secure Shell (SSH)	No	Yes	No
Web (HTTP)	Yes	Yes	No
Secure Web (HTTPS)	Yes	Yes	No
File Shares (CIFS)	Yes	Yes	Yes
Citrix Portal (Citrix)	No	Yes	No

Microsoft Outlook Web Access

SonicWALL SSL-VPN models 2000 and higher include reverse proxy application support for all versions of OWA 2003 and 2007.

Note SonicWALL SSL-VPN 200 supports OWA 2007 light version only.

Microsoft OWA Premium mode is a Web client for Microsoft Outlook 2003/2007 that simulates the Microsoft Outlook interface and provides more features than basic OWA. Microsoft OWA Premium includes features such as spell check, creation and modification of server-side rules, Web beacon blocking, support for tasks, auto-signature support, and address book enhancements. SonicWALL SSL VPN HTTP(S) reverse proxy functionality supports Microsoft OWA Premium.

Microsoft OWA Premium includes the following features:

- Access to email, calendar, and tasks
- New Outlook look-and-feel, including right-click functionality
- Ability to mark an email as unread
- Server-side spelling checker (limited to six languages)
- Forms-based authentication (session time-out)
- S/MIME support

Note S/MIME support for Microsoft OWA Premium is only available on Internet Explorer 6 SP1 or higher.

- Two-line view

- Context menus
- Improved keyboard shortcuts
- Ability to forward meeting requests
- Notifications on navigation pane
- Ability to add to contacts
- Ability to pick names from address book
- Ability to set maximum number of messages displayed in views
- Support for bi-directional layout for Arabic and Hebrew

Note Bi-directional layout support for Arabic and Hebrew for Microsoft OWA Premium is only available on Internet Explorer 6 SP1 or higher.

- Option to set message status “mark as read” when using the reading pane
- Public folders display in their own browser window
- Access to GAL property sheets within an email message or meeting request
- Message sensitivity settings on information bar
- Attendee reminder option for meeting request
- Ability to launch the calendar in its own window
- User interface to set common server-side rules
- Outlook style Quick Flags
- Support for message signatures
- Search folders (must be created in Outlook online mode)
- Deferred search for new messages after delete
- Attachment blocking
- Web beacon blocking to make it more difficult for senders of spam to confirm email addresses
- Protection of private information when a user clicks a hyperlink in the body of an email message

See “Creating Unique Access Policies for AD Groups” on page 295 for a use case involving configuring group-based access policies for multiple Active Directory groups needing access to Outlook Web Access.

Windows Sharepoint Services (version 3.0)

SonicWALL SSL VPN reverse proxy application support for Windows Sharepoint Services 3.0 is supported on SonicWALL SSL-VPN models 2000 and higher, and includes the following features:

- Site Templates
- Wiki Sites
- Blogs
- RSS Feeds
- Project Manager
- Mobile Access to Content
- My Site
- Search Center

- Document Center
- Document Translation Management
- Web Content Management
- Workflows
- Report Center

Note For features that rely on Windows Sharepoint Services-compatible client programs, SSL VPN 4.0 Reverse Proxy does not support client integration capabilities on Internet Explorer.

Single sign-on is supported only for basic authentication.

Only forms-based authentication and basic authentication schemes are supported

Lotus Domino Web Access 7

SonicWALL SSL VPN reverse proxy application support for Domino Web Access 7 is supported on SonicWALL SSL-VPN models 2000 and higher, and includes the following features:

- Email
- Navigation
- Calendar
- Folders and storage
- Contacts
- Tasks and notes
- Rules
- Options and preferences
- Help
- Follow-up reminders

Citrix Portal

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. The Citrix applet requires SUN JRE 1.6.0_10 or higher.

The Citrix ICA Client has been renamed as the Citrix XenApp plugin.

SonicWALL SSL-VPN models 2000 and higher appliances support client computers running Citrix XenApp plugin 11.0 or earlier (including earlier versions of ICA Client) and Citrix Java client 9.6 or earlier. The minimum working version of the Citrix ICA Client for Windows Vista is 10.0.

SonicOS SSL VPN 4.0 supports Citrix XenApp Server 5.0 in addition to support for XenApp/ Presentation Server 4.0, 4.5 and MetaframeXP FR3, supported in previous releases.

SNMP Overview

SonicWALL SSL VPN devices running SSL VPN 4.0 or higher support Simple Network Management Protocol (SNMP), which reports remote access statistics. SNMP support facilitates network management for administrators, allowing them to leverage standardized reporting tools.

DNS Overview

The administrator can configure DNS on the SonicWALL SSL-VPN appliance to enable it to resolve host names with IP addresses. The SonicWALL SSL VPN Web-based management interface allows the administrator to configure a hostname, DNS server addresses, and WINS server addresses.

Network Routes Overview

Configuring a default network route allows your SSL-VPN appliance to reach remote IP networks through the designated default gateway. The gateway will typically be the upstream firewall to which the SSL-VPN appliance is connected. In addition to default routes, it also possible to configure specific static routes to hosts and networks as a preferred path, rather than using the default gateway.

Two-Factor Authentication Overview

Two-factor authentication is an authentication method that requires two independent pieces of information to establish identity and privileges. Two-factor authentication is stronger and more rigorous than traditional password authentication that only requires one factor (the user's password).

SonicWALL's implementation of two-factor authentication partners with two of the leaders in advanced user authentication: RSA and VASCO.

Note Single sign-on (SSO) in SonicWALL SSL VPN does not support two-factor authentication.

See the following sections:

- "Benefits of Two-Factor Authentication" section on page 27
- "How Does Two-Factor Authentication Work?" section on page 28
- "Supported Two-Factor Authentication Providers" section on page 28

Benefits of Two-Factor Authentication

Two-factor authentication offers the following benefits:

- Greatly enhances security by requiring two independent pieces of information for authentication.
- Reduces the risk posed by weak user passwords that are easily cracked.

- Minimizes the time administrators spend training and supporting users by providing a strong authentication process that is simple, intuitive, and automated.

How Does Two-Factor Authentication Work?

Two-factor authentication requires the use of a third-party authentication service. The authentication service consists of two components:

- An authentication server on which the administrator configures user names, assigns tokens, and manages authentication-related tasks.
- Tokens that the administrator gives to users which display temporary token codes.

With two-factor authentication, users must enter a valid temporary passcode to gain access. A passcode consists of the following:

- The user's personal identification number (PIN)
- A temporary token code

Users receive the temporary token codes from their RSA or VASCO token cards. The token cards display a new temporary token code every minute. When the RSA or VASCO server authenticates the user, it verifies that the token code timestamp is current. If the PIN is correct and the token code is correct and current, the user is authenticated.

Because user authentication requires these two factors, the RSA SecureID and VASCO DIGIPASS solution offers stronger security than traditional passwords (single-factor authentication).

Supported Two-Factor Authentication Providers

RSA

RSA is an algorithm for public-key cryptography. RSA utilizes RSA SecurID tokens to authenticate through an RSA Authentication Manager server. RSA is supported on the SSL-VPN 2000 and SSL-VPN 4000 platforms only.

VASCO

VASCO is a public company that provides user authentication products. VASCO utilizes Digipass tokens to authenticate through a VACMAN Middleware server. VASCO is supported on all SonicWALL SSL-VPN platforms.

One Time Password Overview

This section provides an introduction to the One Time Password feature. This section contains the following topics:

What is One Time Password?

SonicWALL SSL VPN One Time Password feature adds a second layer of login security to the standard username and password. A one-time password is a randomly generated, single-use password. The SonicWALL SSL VPN One Time Password feature is a two-factor authentication scheme that utilizes one-time passwords in addition to standard user name and password credentials, providing additional security for SonicWALL SSL VPN users.

The SonicWALL SSL VPN One Time Password feature requires users to first submit the correct SonicWALL SSL VPN login credentials. After following the standard login procedure, the SSL VPN generates a one-time password, which is sent to the user at a pre-defined email address. The user must login to that email account to retrieve the one-time password and type it into the SSL VPN login screen when prompted, before the one-time password expires.

Benefits of One Time Passwords

The SonicWALL SSL VPN One Time Password feature provides more security than single, static passwords alone. Using a one-time password in addition to regular login credentials effectively adds a second layer of authentication. Users must be able to access the email address defined by the SSL VPN administrator before completing the SSL VPN One Time Password login process. Each one-time password is single-use and expires after a set time period, requiring that a new one-time password be generated after each successful login, cancelled or failed login attempt, or login attempt that has timed out, thus reducing the likelihood of a one-time password being compromised.

How Does the SSL VPN One Time Password Feature Work?

The SSL VPN administrator can enable the One Time Password feature on a per-user or per-domain basis. To enable the One Time Password feature on a per-user basis, the administrator must edit the user settings in the SSL VPN management interface. The administrator must also enter an external email address for each user who is enabled for One Time Passwords. For users of Active Directory and LDAP, the administrator can enable the One Time Password feature on a per-domain basis.

Note Enabling the One Time Password feature on a per-domain basis overrides individual “enabled” or “disabled” One Time Password settings. Enabling the One Time Password feature for domains does not override manually entered email addresses, which take precedence over those auto-configured by a domain policy and over AD/LDAP settings.

In order to use the SSL VPN One Time Password feature, the administrator must configure valid mail server settings in the **Log > Settings** page of the SSL VPN management interface. The administrator can configure the One Time Password feature on a per-user or per-domain basis, and can configure timeout policies for users.

If the email addresses to which you want to deliver your SSL VPN One Time Passwords are in an external domain (such as SMS addresses or external webmail addresses), you will need to configure your SMTP server to allow relaying from the SSL-VPN to the external domain.

For information about how to configure Microsoft Exchange to support SSL VPN One Time Password, see the *SonicWALL SSL VPN One Time Password Feature Module*, available online at:

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

For users enabled for the One Time Password feature either on a per-user or per-domain basis, the login process begins with entering standard user name and password credentials in the SSL VPN interface. After login, users receive a message that a temporary password will be sent to a pre-defined email account. The user must login to the external email account and retrieve the one-time password, then type or paste it into the appropriate field in the SSL VPN login interface. Any user requests prior to entering the correct one-time password will re-direct the user to the login page.

The one-time password is automatically deleted after a successful login and can also be deleted by the user by clicking the **Cancel** button in the SSL VPN interface, or will be automatically deleted if the user fails to login within that user's timeout policy period.

Configuring One Time Passwords for SMS-Capable Phones

SonicWALL SSL VPN One Time Passwords can be configured to be sent via email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS (Short Message Service).

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

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T PCS: 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

Tip Refer to "SMS Email Formats" section on page 339 for a more detailed list of SMS email formats.

Note These SMS email formats are for reference only. These email formats are subject to change and may vary. You may 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.

To configure the SonicWALL SSL-VPN appliance to send one-time passwords to an SMS email address, follow the procedure described in the "Editing User Settings" section on page 206, and enter the user's SMS address in the **E-mail address** field.

Verifying Administrator One Time Password Configuration

To verify that an individual user account has been enabled to use the One Time Password feature, login to the SonicWALL SSL VPN Virtual Office user interface using the credentials for that account.

If you are able to successfully login to Virtual Office, you have correctly used the One Time Password feature.

If you cannot login using One Time Password, verify the following:

- Are you able to login without being prompted to check your email for One-time Password? The user account has not been enabled to use the One-time Password feature.
- Is the email address correct? If the email address for the user account has been entered incorrectly, login to the management interface to correct the email address.
- 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 login 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 within the time allotted by the user's timeout policy as set in the **Log > Settings** page.

Virtual Assist Overview

This section provides an introduction to the Virtual Assist feature. Virtual Assist is supported on SSL-VPN 2000 and SSL-VPN 4000 platforms only. This section contains the following topics:

What is Virtual Assist?

Virtual Assist is an easy to use tool that allows SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Providing support to customers is traditionally a costly and time consuming aspect of business. Virtual Assist creates a simple to deploy, easy to use remote support solution.

Benefits of Virtual Assist

Virtual Assist provides the following benefits:

- **Simplified and effective customer support** - Support staff can use Virtual Assist to directly access customers computers to troubleshoot and fix problems. This eliminates the need for customers to try to explain their problems and their computer's behavior over the phone.
- **Time and cost savings** - Virtual Assist eliminates the need for support staff to visit customers to troubleshoot problems and reduces the average time-to-resolution of support calls.
- **Educational tool** - Trainers and support staff can use Virtual Assist to remotely show customers how to use programs and tools.
- **Seamless integration with existing authentication system** - Ensures that the customers are who they say they are. Alternatively, the local database of the SSL-VPN appliance and tokenless two-factor authentication can be utilized.

- **Secure connections** - 256-bit AES SSL encryption of the data by the SSL-VPN appliance provides a secure environment for the data and assists in the effort to be compliant with regulations like Sarbanes-Oxley and HIPAA.
- **Greater flexibility for remote access -** Using the Virtual Access functionality, support staff can access their personal systems located outside the LAN of the SRA appliance.

How Does Virtual Assist Work?

The following sections describe how the Virtual Assist feature works:

Basic Operation

Virtual Assist is a lightweight, thin client that installs automatically using Java from the SonicWALL SSL VPN 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.

Note When a user requests service as a customer, Virtual Assist should not be run while connected to the system via RDP for Windows Vista platforms. Virtual Assist runs as a service for proper access to the customer's system, so correct permissions cannot be set if it is run from an RDP connection.

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 SonicWALL SSL VPN Virtual Office.
2. The technician monitors the Assistance Queue for customers requesting assistance.
3. The customer requests assistance by one of the following methods:
   - Logs into the SonicWALL SSL VPN Virtual Office and clicks on the Virtual Assist 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.
4. The Virtual Assist application installs and runs on the customer's browser.
5. The customer appears in the Virtual Assist Assistance Queue.
6. The technician clicks on the customer's name and launches a Virtual Assist session.
7. The customer clicks on a warning pop-up window that gives the technician control over the customer's computer.
8. The technician's Virtual Assist window now displays the customer's 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 performs.
9. If at anytime the customer wants to end the session, they can take control and click on the **End Virtual Assist** button in the bottom right corner of the screen.

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

Remote File Transfer

Virtual Assist includes a Remote File Transfer feature that enables the technician to transfer files directly to and from the customer's computer. The technician launches the File Transfer process by clicking a button in the Virtual Assist taskbar in the top left corner of the Virtual Assist window. The File Transfer feature supports the upload and download of multiple files.

Chat Feature

Virtual Assist includes a chat feature that allows the technician and customer to communicate using an instant message-style chat function. Either the technician or the customer can initiate a chat session by clicking on the **Chat** button in the Virtual Assist taskbar.

Email Invitation

From the technician view of Virtual Assist, technicians can send email invitations to customers that contain a direct URL link to initiate a Virtual Assist session. The technician can optionally include a unique message to the customer. When the customer clicks on the email link to Virtual Assist, only the technician who sent the invitation can assist that customer.

Virtual Access

Virtual Access, as part of the larger Virtual Assist feature, allows technicians to gain access to their personal systems outside the LAN of the SRA appliance. After downloading and installing a client from the portal page for Virtual Access mode, the personal system will appear only on that technician's Virtual Assist support queue, within the SRA's management interface. While Virtual Access must be enabled per-portal, this functionality provides greater remote access flexibility for support technicians.

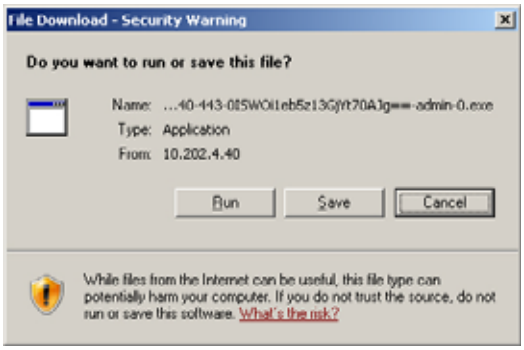
Launching a Virtual Assist Technician Session

To launch a Virtual Assist session as a technician, perform the following steps.

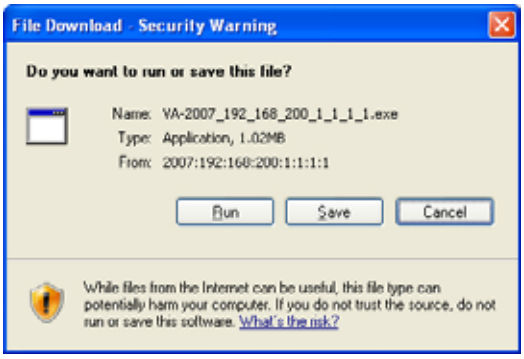
Step 1 Log in to the SonicWALL SSL-VPN security appliance Virtual Office. If you are already logged in to the SonicWALL SSL VPN customer interface, click on the **Virtual Office** button.

Step 2 Click on the **Virtual Assist** button.

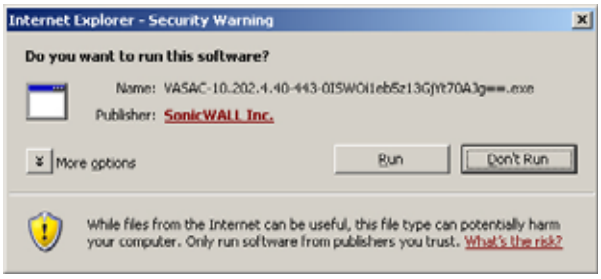
Step 3 The File Download window displays, and Virtual Assist attempts to automatically install. Click **Run** to launch the program directly, or click **Save** to save the installer file to your computer, and then manually launch it.



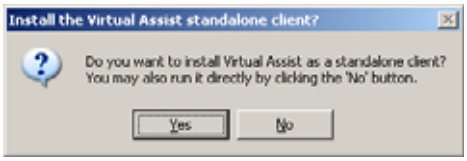
When downloading through IPv6, the File Download window displays IPv6 information.



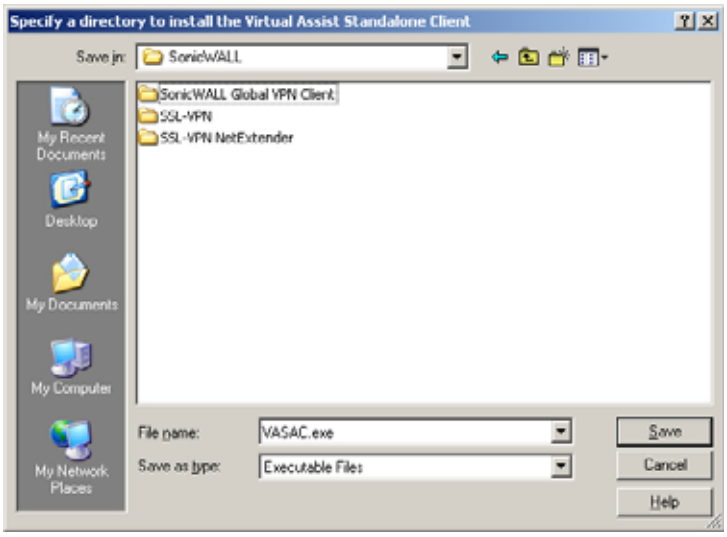
Step 4 When you launch the installer, you may see an additional warning message. Click **Run**.



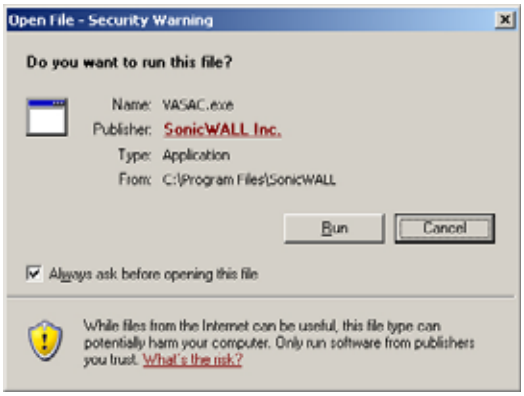
Step 5 A pop-up window asks if you would like to install Virtual Assist as a standalone client. Click **Yes** to save the application. A shortcut will be added to your desktop and a link to the application will be added to the program list on your Start Menu. Click **No** to launch Virtual Assist without saving the application for future use.



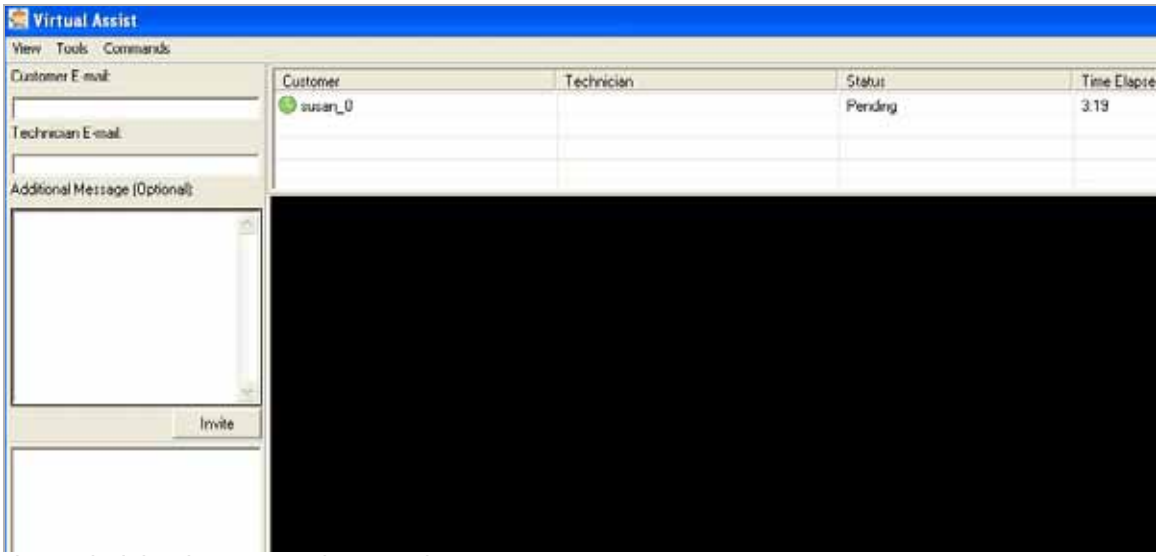
Step 6 If you clicked **Yes** to save the application, you will be prompted to select a location to save the file. Select an appropriate location, such as C:\Program Files\SonicWALL.



Step 7 When Virtual Assist launches for the first time, you may see a security warning pop-up window. De-select the **Always ask before opening this file** checkbox to avoid this window in the future. Click **Run**.



Step 8 The Virtual Assist standalone application launches.



Step 9 The technician is now ready to assist customers.

Performing Virtual Assist Technician Tasks

To get started, the technician logs into the SonicWALL SSL-VPN appliance and launches the Virtual Assist application.

Note Each technician can only assist one customer at a time.

Once the technician has launched the Virtual Assist application, the technician can assist customers by performing the following tasks:

- “Inviting Customers by Email” on page 37
- “Assisting Customers” on page 37
- “Using the Virtual Assist Taskbar” on page 38
- “Controlling the Virtual Assist Display” on page 39
- “Using the Virtual Assist File Transfer” on page 40

Inviting Customers by Email

Step 1 To invite a customer to Virtual Assist, use the email invitation form on the left of the Virtual Assist window.

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.

Step 2 Enter the customer's email address in the **Customer E-mail** field.

Step 3 Optionally, enter **Technician E-mail** to use a different return email address than the default technician email.

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

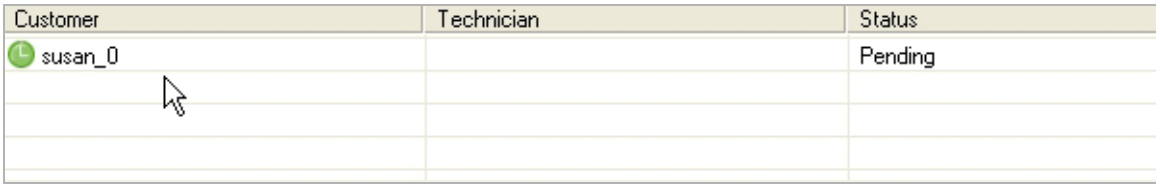
Step 5 Click **Invite**. The customer will receive an email with an HTML link to launch Virtual Assist.

Step 6 Customers requesting assistance will appear in the Assistance Queue, and the duration of time they have been waiting will be displayed.

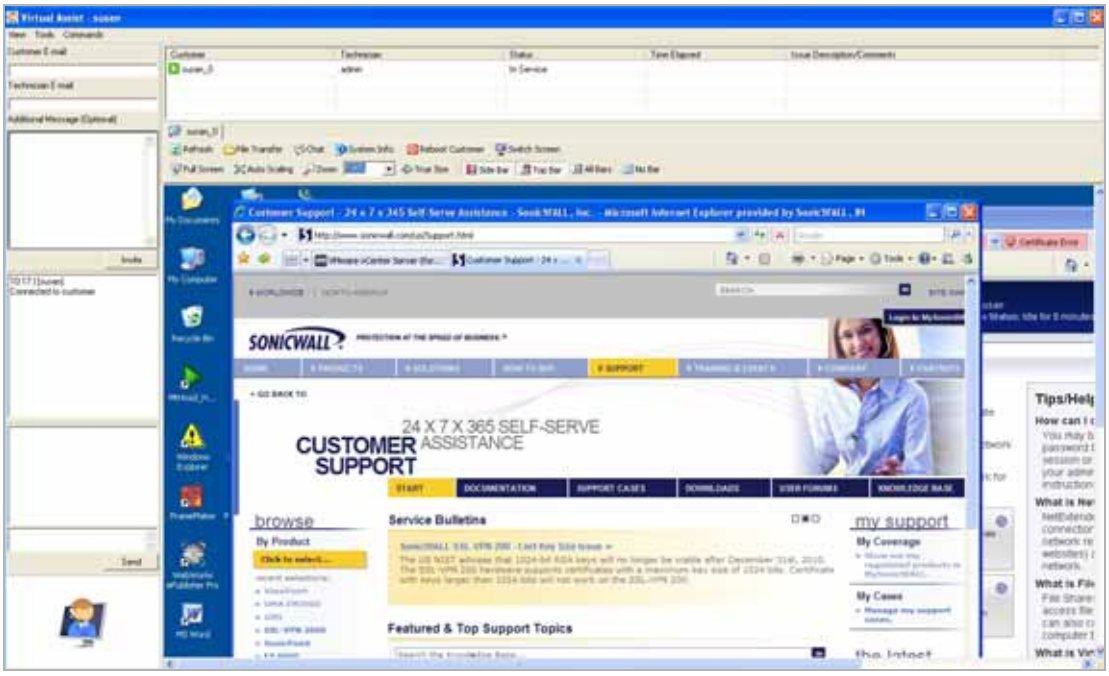
Assisting Customers

Step 1 A pop-up window in the lower right task bar alerts the technician when a customer is in the assistance queue.

Step 2 Double-click on a customer's user name to begin assisting the customer.



Step 3 The customer's entire desktop is displayed in the bottom right window of the 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 performs.

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 may cause confusion and consternation if they both attempt "to drive" at the same time.

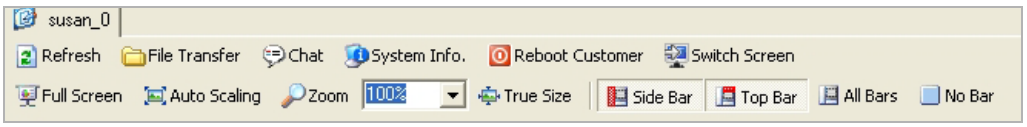
The customer has a small tool bar in the bottom right of their screen, with three options.

The customer has the following options during a Virtual Assist session, each enabled after clicking the corresponding button.

- **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.

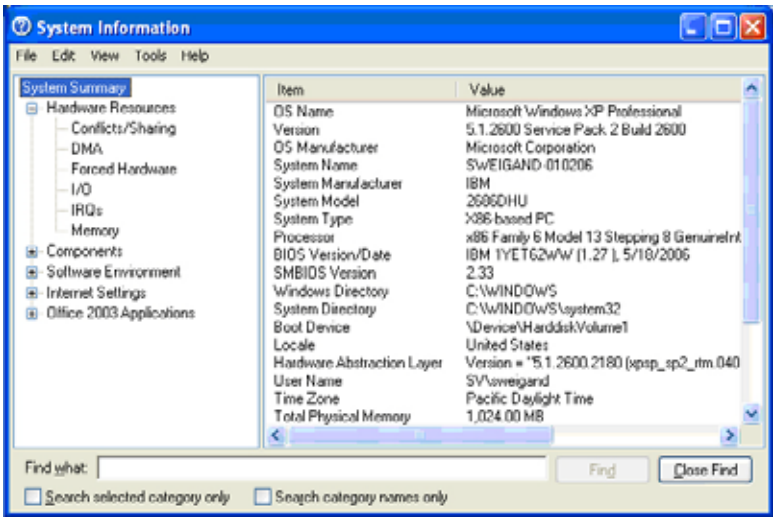
Using the Virtual Assist Taskbar

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



- **Refresh** - R Refreshes the display of the customer's computer.
- **File Transfer** - Launches a window to transfer files to and from the customer's computer. See the "Using the Virtual Assist File Transfer" section on page 40 for more information.
- **Chat** - Launches the chat window to communicate with the customer. The technician can also use the dedicated chat window in the bottom left window of the Virtual Assist application.

- **System Info** -Displays detailed information about the customer's computer.



- **Reboot Customer** - Reboot the customer's computer. Unless you have Requested full control, the customer will be warned about and given the opportunity to deny the reboot.
- **Switch Screen** - Switches to a second monitor if the customer's computer has more than one monitor configured.

Controlling the Virtual Assist Display

- **Full Screen** - Hides all of the Virtual Assist toolbars and displays the customer's desktop on the technician's entire screen with the Virtual Assist taskbar in the top left corner.

  If the Virtual Assist taskbar doesn't display, move your mouse to the top middle of the screen. Right-click on the taskbar and click **Restore** to exit full-screen mode.
- **Auto Scaling** - Zooms the display to fill the entire Virtual Assist window.
- **Zoom** - Zooms the display to one of several presets or allows you enter a specific value.
- **True Size** - Zooms to 100%.
- **Side Bar** - Toggles the display of the side bar with the email invitation and chat windows.
- **Top Bar** - Toggles the display of the top bar with the customer queue and toolbar.
- **All Bars** - Displays both the side bar and top bar.
- **No Bar** - Hides both the side bar and top bar.

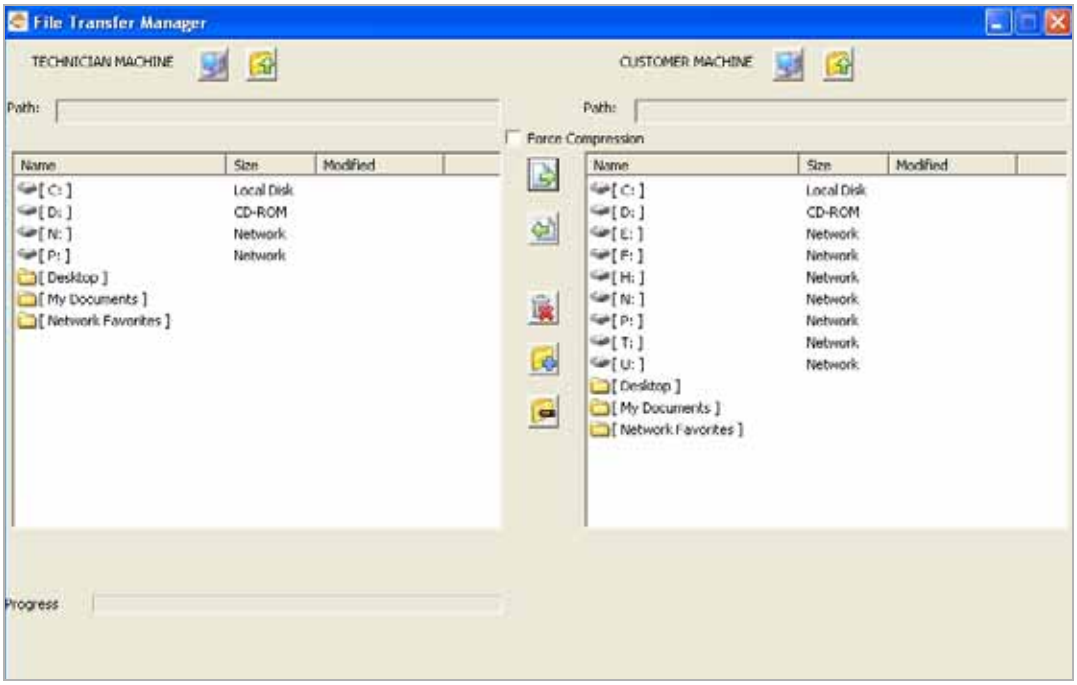
Note A number of these options can be configured from the pull-down menus at the top of the Virtual Assist application.

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 will appear on the customer's desktop.

Using the 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 over-writing files, the customer is warned and must give the technician permission unless the technician has elected **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 the **Exit** button 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 the **Ctrl** button while clicking on the files.

Enabling a System for Virtual Access

If Virtual Access has been enabled on the Virtual Assist tab on the Portals > Portals page of the management interface, users should see a link on the portal to set-up a system for Virtual Access. To enable Virtual Access within the SRA management interface, see "Configuring Per-Portal Virtual Assist Settings" on page 114. The following process allows Virtual Access to bet set-up on a system.

Step 1 Login to the portal through the system you wish to set-up for Virtual Access and click the Virtual Access link.

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

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

Step 3 Fill in the necessary information in the provided fields to set-up the system in 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://").
- **Portal:** The name of the portal the technician would normally login to.
- **Computer Name:** This is an identifier for the system to help differentiate between other systems that may be waiting for support in the queue.

- **Password:** This is a password the technician must enter prior to accessing the system through the support queue.

Step 4 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 Virtual Assist > Status page within the management interface.Upon double-clicking the system listing, the technician will be prompted to provide the password established during system set-up to gain Virtual Access to the system.

Ending Virtual Access Mode

Disconnecting from a Virtual Access session will place the system back in the support queue for later access by the technician. From the personal system-side, the user/technician may uninstall or terminate the application from the tray option icons.

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

Note For tasks and information on using Virtual Assist as an end-user, refer to the *SonicWALL SSL VPN User's Guide*.

Web Application Firewall Overview

This section provides an introduction to the Web Application Firewall feature. Web Application Firewall is supported on SSL-VPN 2000 and SSL-VPN 4000 platforms only. This section contains the following topics:

What is Web Application Firewall?

Web Application Firewall is subscription-based software that runs on the SonicWALL SSL-VPN appliance and protects Web applications running on servers behind the SSL-VPN. Web Application Firewall also provides real-time protection for resources such as HTTP(S) bookmarks, Citrix bookmarks, offloaded Web applications, and the SSL-VPN management interface and user portal that run on the SonicWALL SSL-VPN appliance itself.

Web Application Firewall provides real-time protection against a whole suite of Web attacks such as Cross-site scripting, SQL Injection, OS Command Injection, and many more. The top ten vulnerabilities for Web applications are tracked by OWASP, an open source community that focuses its efforts on improving the security of Web applications. SonicOS SSL VPN Web Application Firewall protects against these top ten, defined in 2007 as follows:

Table 4 OWASP Top Ten Vulnerabilities

Name	Description
A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a Web browser without first validating or encoding that content. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface Web sites, and possibly introduce worms.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in Web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

Name	Description
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable Web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the Web application that it attacks.
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

In addition to the top ten threats listed above, Web Application Firewall protects against Slowloris HTTP Denial of Service attacks. This means that Web Application Firewall also protects all the backend Web servers against this attack. Many Web servers, including Apache, are vulnerable to Slowloris. Slowloris is especially effective against Web servers that use threaded processes and limit the amount of threading allowed.

Slowloris is a stealthy, slow-acting attack that sends partial HTTP requests at regular intervals to hold connections open to the Web server. It gradually ties up all the sockets, consuming sockets as they are freed up when other connections are closed. Slowloris can send different host headers, and can send GET, HEAD, and POST requests. The string of partial requests makes Slowloris comparable to a SYN flood, except that it uses HTTP rather than TCP. Only the targeted Web server is affected, while other services and ports on the same server are still available. When the attack is terminated, the Web server can return to normal within as little as 5 seconds, making Slowloris useful for causing a brief downtime or distraction while other attacks are initiated. Once the attack stops or the session is closed, the Web server logs may show several hundred 400 errors.

For more information about how Web Application Firewall protects against the OWASP top ten and Slowloris types of attacks, see the “How Does Web Application Firewall Work?” section on page 45.

Web Application Firewall can also protect an offloaded Web application, which is a special purpose portal created to provide seamless access to a Web application running on a server behind the SSL-VPN appliance. The portal must be configured as a virtual host. It is possible to disable authentication and access policy enforcement for such an offloaded host. If

authentication is enabled, a suitable domain needs to be associated with this portal and all SonicWALL advanced authentication features such as One Time Password, Two-factor Authentication, and Single Sign-On apply to the offloaded host.

Benefits of Web Application Firewall

Web Application Firewall is secure and can be used in various areas, including financial services, healthcare, application service providers, and e-commerce. SonicOS SSL VPN uses SSL encryption to encrypt data between the Web Application Firewall and the client. SonicOS SSL VPN also satisfies OWASP cryptographic storage requirements by encrypting keys and passwords wherever necessary.

Companies using Web Application Firewall can reduce the development cost required to create secure applications and also cut out the huge turnaround time involved in deploying a newly found vulnerability fix in every Web application by signing up for Web Application Firewall signature updates.

Resources accessed over Application Offloaded portals and HTTP(S) bookmarks can be vulnerable due to a variety of reasons ranging from badly designed architecture to programming errors. Web Application Firewall provides an effective way to prevent a hacker from exploiting these vulnerabilities by providing real-time protection to Web applications deployed behind the SonicWALL SSL-VPN appliance.

Deploying Web Application Firewall at the SSL-VPN appliance lets network administrators use application offloading even when it exposes Web applications needing security to internal and remote users. Application offloading avoids URL rewriting, which improves the proxy performance and functionality.

There are several benefits of integrating Web Application Firewall with SonicWALL SSL-VPN appliances. Firstly, identity-based policy controls are core to Web Application Firewall and this is easily achievable using SSL VPN technology. Secondly, there are lower latencies due to the existing hardware-based SSL offloading. Most importantly, SSL-VPN appliances run Web applications and must be protected from such attacks.

As small businesses adopt hosted services to facilitate supplier collaboration, inventory management, online sales, and customer account management, they face the same strict compliance requirements as large enterprises. Web Application Firewall on a SonicWALL SSL-VPN appliance provides a convenient, cost-effective solution.

Web Application Firewall is easy to configure in the SonicWALL SSL-VPN management interface. The administrator can configure Web Application Firewall settings globally, by attack priority, and on a per-signature basis. Once custom configuration settings or exclusions are in place, you can disable Web Application Firewall without losing the configuration, allowing you to perform maintenance or testing and then easily re-enable it.

How Does Web Application Firewall Work?

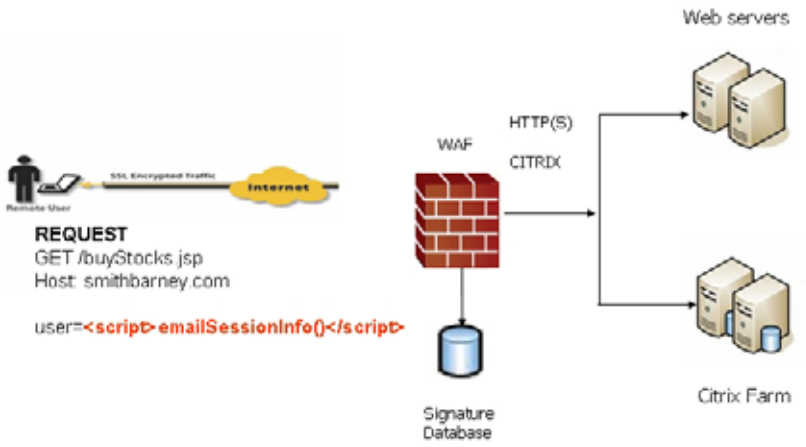
To use the Web Application Firewall feature, the administrator must first license the software or start a free trial. Web Application Firewall must then be enabled on the Web Application Firewall > Settings page of the SonicWALL SSL-VPN management interface.Web Application Firewall can be configured to log or block detected attacks arriving from the Internet.

The following sections describe how Web Application Firewall and SonicOS SSL VPN prevent attacks such as those listed in the OWASP top ten:

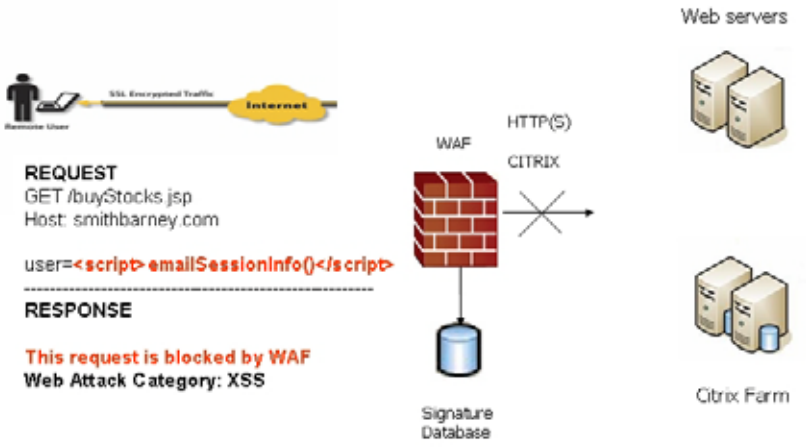
- “How are Signatures Used to Prevent Attacks?” on page 46
- “How is Cross-Site Request Forgery Prevented?” on page 47

How are Signatures Used to Prevent Attacks?

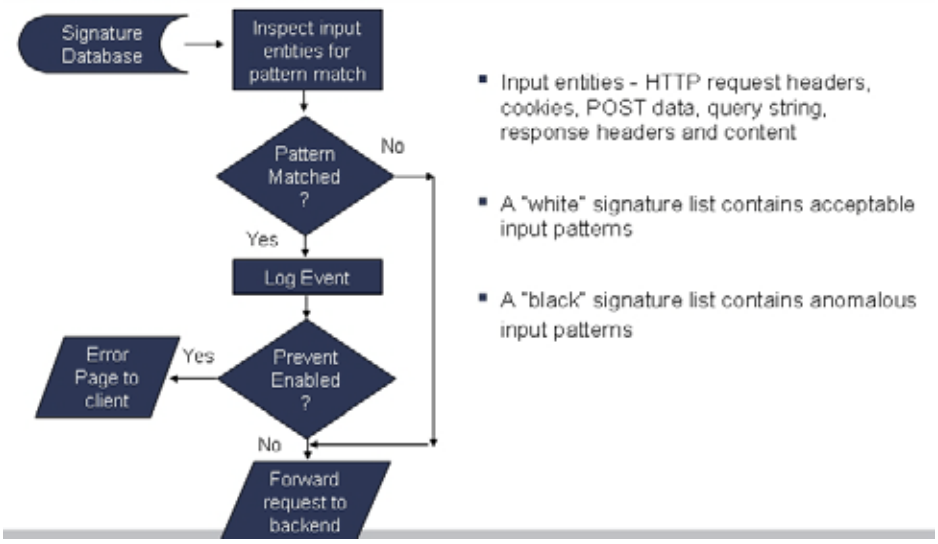
For Cross Site Scripting, Injection Flaws, Malicious File Execution, and Insecure Direct Object Reference vulnerabilities, the Web Application Firewall feature uses a black list of signatures that are known to make Web applications vulnerable. New updates to these signatures are periodically downloaded from a SonicWALL signature database server, providing protection from recently introduced attacks.



When input arrives from the Internet, Web Application Firewall inspects HTTP/HTTPS request headers, cookies, POST data, query strings, response headers, and content. It compares the input to both a black list and a white list of signatures. If pattern matching succeeds for any signature, the event is logged and/or the input is blocked if so configured. If blocked, an error page is returned to the client and access to the resource is prevented. If blocked, an error page is returned to the client and access to the resource is prevented. The threat details are not exposed in the URL of the error page. If configured for detection only, the attack is logged but the client can still access the resource. If no signature is matched, the request is forwarded to the Web server for handling.



The Web Application Firewall process is outlined in the following flowchart.



In the case of a blocked request, the following error page is returned to the client:

This page is customizable under Web Application Firewall > Settings in the SSL-VPN management interface. Some administrators may want to customize the HTML contents of this page. Others may not want to present a user friendly page for security reasons. Instead, they may prefer the option to present an HTTP error code such as 404 (Not found) or 403 (Access Denied).

How is Cross-Site Request Forgery Prevented?

CSRF attacks are not detected with signature matching. Using this vulnerability, a hacker disguised as the victim can gain unauthorized access to application even without stealing the session cookie of a user. While a victim user is authenticated to a Web site under attack, the user may unwittingly load a malicious Web page from a different site within the same browser process context, for instance, by launching it in a new tab part of the same browser window. If this malicious page makes a hidden request to the victim Web server, the session cookies in the browser memory are made part of this request making this an authenticated request. The Web server serves the requested Web page as it assumes that the request was a result of a user action on its site. To maximize the benefits, typically, hackers targets actionable requests, such as data updates to carry out this attack.

To prevent CSRF attacks, every HTTP request within a browser session needs to carry a token based on the user session. To ensure that every request carries this token, the Web Application Firewall feature rewrites all URLs contained in a Web page similarly to how they are rewritten by the Reverse Proxy for HTTP(S) Bookmarks feature. If CSRF protection is enabled, this is also performed for Application Offloading.

How is Information Disclosure Prevented?

Web Application Firewall prevents Information Disclosure and Improper Error Handling by providing a way for the administrator to configure text containing confidential and sensitive information so that no Web site accessed through the Web Application Firewall reveals this text. These text strings are entered on the Web Application Firewall > Settings page.

Beside the ability to pattern match custom text, signatures pertaining to information disclosure are also used to prevent these types of attacks.

The Web Application Firewall > Settings page also allows the administrator to configure the global idle session timeout. It is highly recommended that this timeout value is kept as low as possible.

How are Broken Authentication Attacks Prevented?

The requirement for Broken Authentication and Session Management requires Web Application Firewall to support strong session management to enhance the authorization requirements for Web sites. SonicOS SSL VPN already has strong authentication capabilities with the ability to support One Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication.

For Session Management, Web Application Firewall pops up a session logout dialog box when the user portal is launched or when a user logs into an application offloaded portal. This feature is enabled by default when Web Application Firewall is licensed and can be disabled from the Web Application Firewall > Settings page.

How are Insecure Storage and Communications Prevented?

Insecure Cryptographic Storage and Insecure Communications are prevented by encrypting keys and passwords wherever necessary, and by using SSL encryption to encrypt data between the Web Application Firewall and the client. SonicOS SSL VPN also supports HTTPS with the backend Web server.

How is Access to Restricted URLs Prevented?

SonicOS SSL VPN supports access policies based on host, subnet, protocol, URL path, and port to allow or deny access to Web sites. These policies can be configured globally or for users and groups.

How are Slowloris Attacks Prevented?

Slowloris attacks can be prevented if there is an upstream device, such as a SonicWALL SSL-VPN security appliance, that limits, buffers, or proxies HTTP requests. Web Application Firewall uses a rate-limiter to thwart Slowloris HTTP Denial of Service attacks.

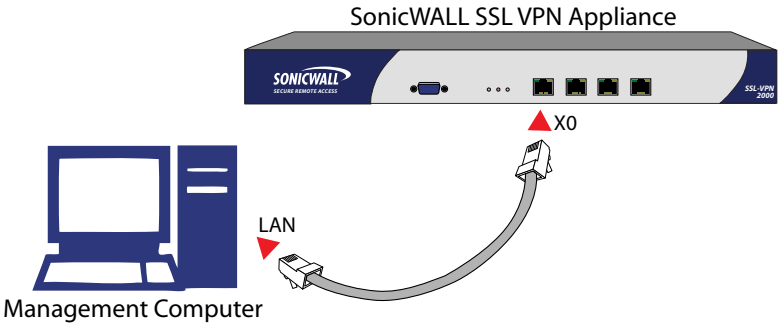
Navigating the SSL VPN Management Interface

The following sections describe how to navigate the SSL VPN management interface:

Management Interface Introduction

The following is an overview of basic setup tasks that connect you to the Web-based management interface of the SonicWALL SSL-VPN appliance. For more detailed information on establishing a management session and basic setup tasks, refer to the *SonicWALL SSL VPN Getting Started Guide*. To access the Web-based management interface of the SonicWALL SSL VPN:

Step 1 Connect one end of a CAT-5 cable into the **X0** port of your SonicWALL SSL-VPN appliance. Connect the other end of the cable into the computer you are using to manage the SonicWALL SSL-VPN appliance.



Step 2 Set the computer you use to manage your SonicWALL SSL-VPN appliance to have a static IP address in the **192.168.200.x/24** subnet, such as **192.168.200.20**. For help with setting up a static IP address on your computer, refer to the *SonicWALL SSL VPN Getting Started Guide* for your model.

Note For configuring the SonicWALL SSL VPN using the Web-based management interface, a Web browser supporting Java and HTTP uploads, such as Internet Explorer 8.0 or higher, Mozilla Firefox 11.0 or higher, or Google Chrome 18.0 or higher, is recommended. Users will need to use Internet Explorer 8.0 or higher, supporting JavaScript, Java, cookies, SSL and ActiveX in order to take advantage of the full suite of SonicWALL SSL VPN applications.

Step 3 Open a Web browser and enter **https://192.168.200.1** (the default LAN management IP address) in the **Location** or **Address** field.

Step 4 A security warning may appear. Click the **Yes** button to continue.

Step 5 The **SonicWALL SSL VPN Management Interface** is displayed and prompts you to enter your user name and password. Enter **admin** in the **User Name** field, **password** in the **Password** field, select **LocalDomain** from the **Domain** drop-down list and click the **Login** button.

Note The number and duration of login attempts can be controlled by the use of the SonicWALL SSL VPN auto-lockout feature. For information on configuring the auto-lockout feature, refer to the "Configuring Login Security" section on page 79.

When you have successfully logged in, you will see the default page, **System > Status**.

Note If the default page after logging in is the Virtual Office user portal, you have selected a domain with user-only privileges. Administration can only be performed from the LocalDomain authentication domain. If you wish to log in as an administrator, make sure you select **LocalDomain** from the **Domain** drop-down list in the **Login** screen.

The **System**, **Network**, **Portals**, **NetExtender**, **Virtual Assist**, **Web Application Firewall**, **Users** and **Log** menu headings on the left side of the browser window configure administrative settings. When you click one of the headings, its submenu options are displayed below it. Click on submenu links to view the corresponding management pages.

The **Virtual Office** option in the navigation menu opens a separate browser window that displays the login page for the user portal, Virtual Office.

The **Help** button in the upper right corner of the management interface opens a separate browser window that displays SonicWALL SSL VPN help.

The **Logout** button in the upper right corner of the management interface terminates the management session and closes the browser window.

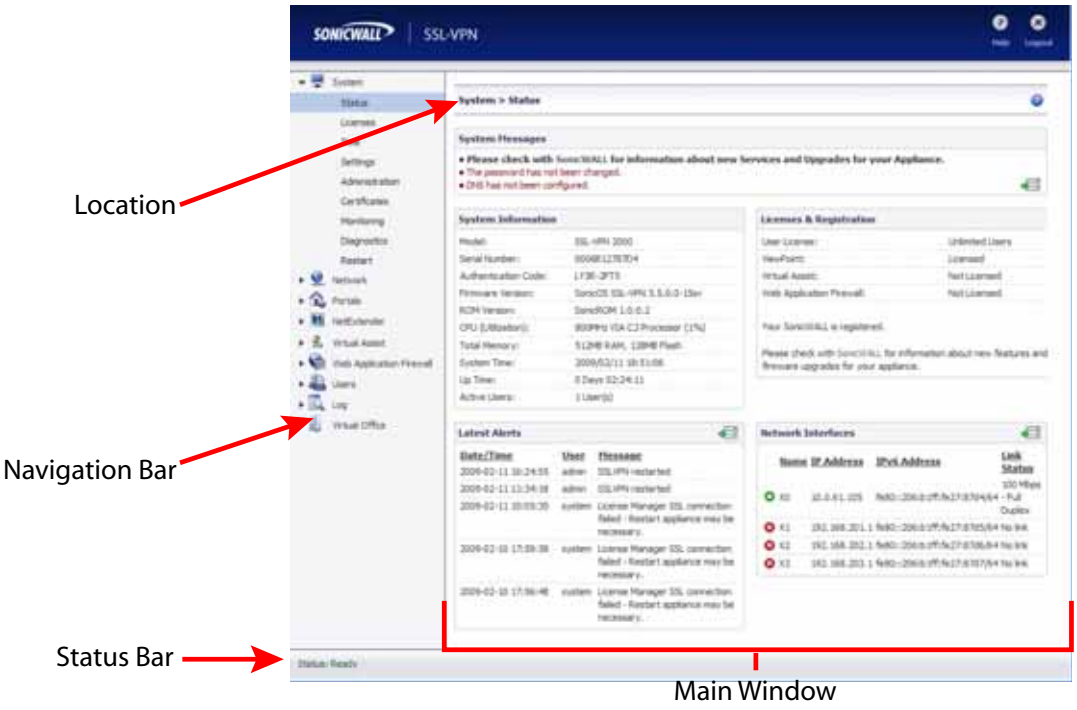
Navigating the Management Interface

The SonicWALL SSL VPN Web-based management interface allows the administrator to configure the SonicWALL SSL-VPN appliance. The management interface contains two main types of objects:

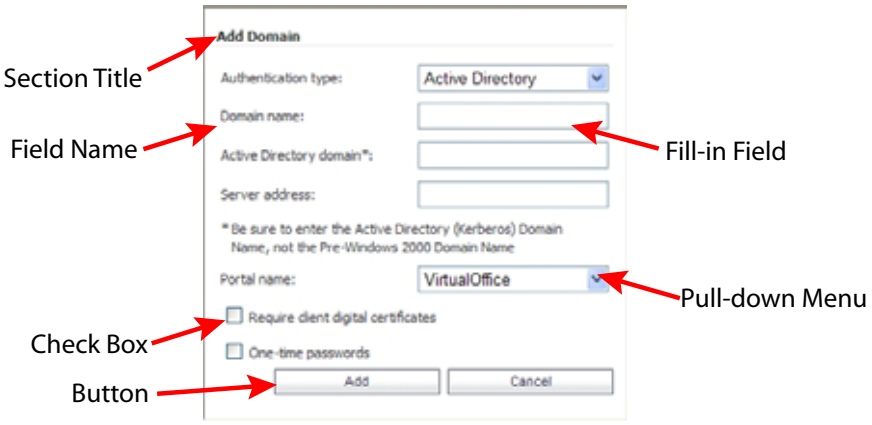
- Windows - Displays information in a read-only format.
- Dialog boxes - Enables administrator interaction to add and change values that characterize objects. For example, IP addresses, names, and authentication types.

Figure 3 is a sample window in the Web-based management interface. Note the various elements of a standard SonicWALL interface window.

Figure 3 System > Status Page



The following is a sample dialog box:



For descriptions of the elements in the management interface, see the following sections:

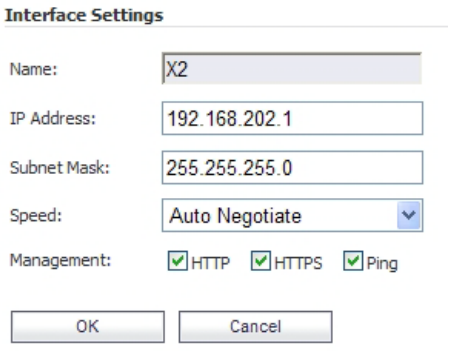
Status Bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicWALL management interface.

Accepting Changes

Click the **Accept** button at the top right corner of the main window to save any configuration changes you made on the page.

If the settings are contained in a secondary window or dialog box within the management interface, the settings are automatically applied to the SonicWALL SSL-VPN appliance when you click **OK**.



Navigating Tables

Navigating tables with large number of entries is simplified by navigation buttons located on the upper right corner of the table. For example, the **Log > View** page contains an elaborate bank of navigation buttons:

Figure 4 Log > View

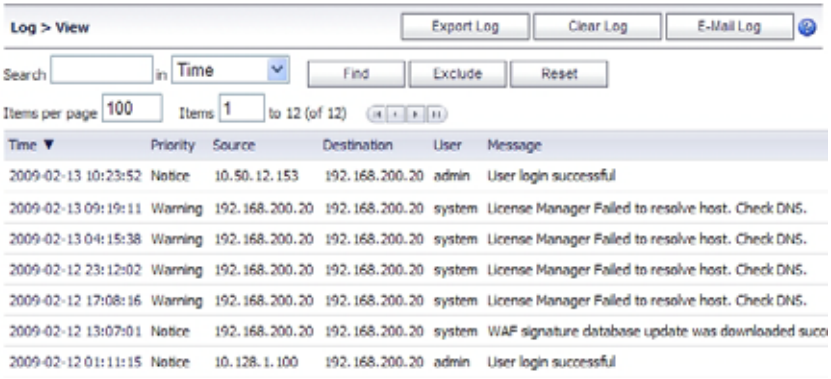


Table 5 Navigation Buttons in the Log View Page

Navigation Button	Description
Find	Allows the administrator to search for a log entry containing the content specified in the Search field. The search is applied to the element of the log entry specified by the selection in the drop-down list. The selections in the drop-down list correspond to the elements of a log entry as designated by the column headings of the Log > View table. You can search in the Time, Priority, Source, Destination, User, and Message elements of log entries.
Exclude	Allows the administrator to display log entries excluding the type specified in the drop-down list.
Reset	Resets the listing of log entries to their default sequence.
Export Log	Allows the administrator to export a log.
Clear Log	Allows the administrators clear the log entries.

Restarting

The System > Restart page provides a Restart button for restarting the SonicWALL SSL-VPN appliance.

Note Restarting takes approximately 2 minutes and causes all users to be disconnected.

Common Icons in the Management Interface

The following icons are used throughout the SonicWALL management interface:

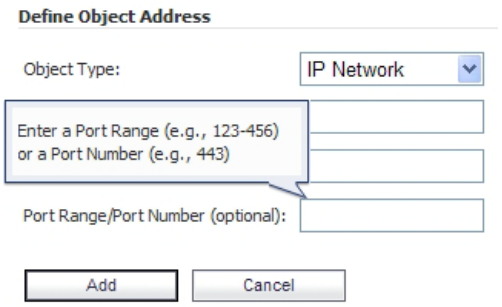
Clicking on the configure icon displays a window for editing the settings.

Clicking on the delete icon deletes a table entry

Moving the pointer over the comment icon displays text from a **Comment** field entry.

Tooltips in the Management Interface

Many pages throughout the management interface display popup tooltips with configuration information when the mouse cursor hovers over a checkbox, text field, or radio button. Some fields have a Help icon that provides a tooltip stating related requirements.



Getting Help

The **Help** button in the upper right corner of the management interface opens a separate Web browser that displays the main SonicWALL SSL VPN help.

SonicWALL SSL VPN also includes online context-sensitive help, available from the management interface by clicking the question mark button on the top-right corner of most pages. Clicking on the question mark button opens a new browser window that displays management page or feature-specific help.

Note Accessing the SonicWALL SSL-VPN appliance online help requires an active Internet connection.

Logging Out

The **Logout** button in the upper right corner of the management interface terminates the management session.

When you click the Logout button, you are logged out of the SonicWALL SSL VPN management interface and the Web browser is closed.

Navigation Bar

The SonicWALL navigation bar is located on the left side of the SonicWALL SSL VPN management interface and is comprised of a hierarchy of menu headings. Most menu headings expand to a submenu of related management functions, and the first submenu item page is

automatically displayed. For example, when you click the **System** heading, the **System > Status** page is displayed. The navigation menu headings are: **System**, **Network**, **Portals**, **NetExtender**, **Virtual Assist**, **Web Application Firewall**, **Users**, **Log**, and **Virtual Office**.

The submenus of each heading on the navigation bar are described briefly in Table 6.

Table 6 SonicWALL SSL VPN Navigation Bar Layout

Tab	Submenu	Action
System	Status	View status of the appliance.
	Licenses	View, activate, and synchronize licenses with the SonicWALL licensing server for Nodes and Users, Virtual Assist, and ViewPoint.
	Time	Configure time parameters.
	Settings	Import, export, and store settings.
	Administration	Configure login security and GMS settings.
	Certificates	Import or generate a certificate.
	Monitoring	View graphs of bandwidth usage, active concurrent users, CPU utilization, and memory utilization.
	Diagnostics	Run diagnostics sessions.
	Restart	Restart the system.
Network	Interfaces	Configure interfaces on the appliance.
	DNS	Configure the appliance to resolve domain names.
	Routes	Set default and static routes.
	Host Resolution	Configure network host name settings.
	Network Objects	Create reusable entities that bind IP addresses to services.
Portals	Portals	Create a customized landing page to your users when they are redirected to the SonicWALL SSL VPN for authentication.
	Application Offloading	This page provides information about offloading a Web application.
	Domains	Create authentication domains that enable you to create access policies.
	Custom Logos	This page informs you that Custom Logos may now be uploaded per portal on the Portals > Portals page, by editing a Portal and selecting the Logo tab.
NetExtender	Status	View active NetExtender sessions.
	Client Settings	Create client addresses for use with the NetExtender application.
	Client Routes	Create client routes for use with the NetExtender application.
Virtual Assist	Status	View active Virtual Assist customer requests.
	Settings	Configure Virtual Assist email, ticket, and queue options, and Assistance code settings.

Tab	Submenu	Action
	Log	View log entries for technician and customer actions, and export, email, or clear the log.
	Licensing	View and configure current Virtual Assist license information.
Web Application Firewall	Status	View status of the Web Application Firewall license and signature database. View a clickable list of threats that were detected or prevented.
	Settings	Enable Web Application Firewall, configure global settings for different priority attacks, global exclusions, per-signature protection levels, and per-signature exclusions.
	Log	View log entries for detected or prevented attacks. Click on a log instance to display additional information about the signature match, signature id, threat name, and other information.
	Licensing	View and configure current Web Application Firewall license information.
Users	Status	View status of users and groups.
	Local Users	Configure local users.
	Local Groups	Configure local groups.
Log	View	View syslog entries that have been generated by the appliance. Export, email, or clear the log.
	Settings	Configure settings for the log environment.
	ViewPoint	Configure SonicWALL ViewPoint server for reporting.
Virtual Office	N/A	Access the Virtual Office portal home page.

Deployment Guidelines

This sections provides information about deployment guidelines for the SonicWALL SSL-VPN appliance. This section contains the following subsections:

Support for Numbers of User Connections

The following table lists the maximum and recommended numbers of concurrent tunnels supported for each appliance.

Appliance Model	Maximum Concurrent Tunnels Supported	Recommended Number of Concurrent Tunnels
SSL-VPN 4000	250	200
SSL-VPN 2000	125	50

For optimal performance, SonicWALL recommends that the number of concurrent tunnels be limited to fewer than, 50 for the SonicWALL SSL-VPN 2000 appliance and approximately 200 for the SonicWALL SSL-VPN 4000 appliance. Factors such as the complexity of applications in use and the sharing of large files can impact performance.

Resource Type Support

The following table describes the types of applications or resources you can access for each method of connecting to the SonicWALL SSL-VPN appliance.

Access Mechanism	Access Types
Standard Web browser	• Files and file systems, including support for FTP and Windows Network File Sharing • Web-based applications • Microsoft Outlook Web Access and other Web-enabled applications • HTTP and HTTPS intranets
SonicWALL NetExtender	• Any TCP/IP based application including: – Email access through native clients residing on the user's laptop (Microsoft Outlook, Lotus Notes, etc.) – Commercial and home-grown applications • Flexible network access as granted by the network administrator
Downloadable ActiveX or Java Client	• An application installed on desktop machines or hosted on an application server, remote control of remote desktop or server platforms • Terminal services, RDP, VNC, Telnet, SSH, and Citrix

Integration with SonicWALL Products

The SonicWALL SSL-VPN appliance integrates with other SonicWALL products, complementing the SonicWALL NSA, PRO and TZ Series product lines. Incoming HTTPS traffic is redirected by a SonicWALL firewall appliance to the SonicWALL SSL-VPN appliance. The SonicWALL SSL-VPN appliance then decrypts and passes the traffic back to the firewall where it can be inspected on its way to internal network resources.

Typical Deployment

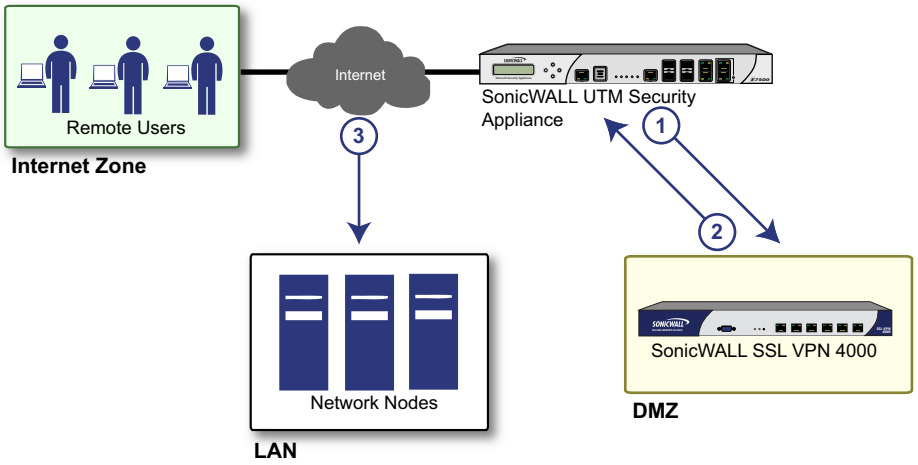
The SonicWALL SSL-VPN is commonly deployed in tandem in "one-arm" mode over the DMZ or Opt interface on an accompanying gateway appliance, for example, a SonicWALL UTM (Unified Threat Management) appliance, such as a SonicWALL NSA 4500.

This method of deployment offers additional layers of security control plus the ability to use SonicWALL's Unified Threat Management (UTM) services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering and Intrusion Prevention, to scan all incoming and outgoing NetExtender traffic.

The primary interface (X0) on the SonicWALL SSL-VPN connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SonicWALL SSL-VPN appliance (step 1). SonicWALL SSL VPN decrypts the session and

determines the requested resource. The SonicWALL SSL VPN session traffic then traverses the gateway appliance (step 2) to reach the internal network resources. While traversing the gateway, security services, such as Intrusion Prevention, Gateway Anti-Virus and Anti-Spyware inspection can be applied by appropriately equipped gateway appliances. The internal network resource then returns the requested content to the SonicWALL SSL-VPN appliance through the gateway (step 3) where it is encrypted and returned to the client.

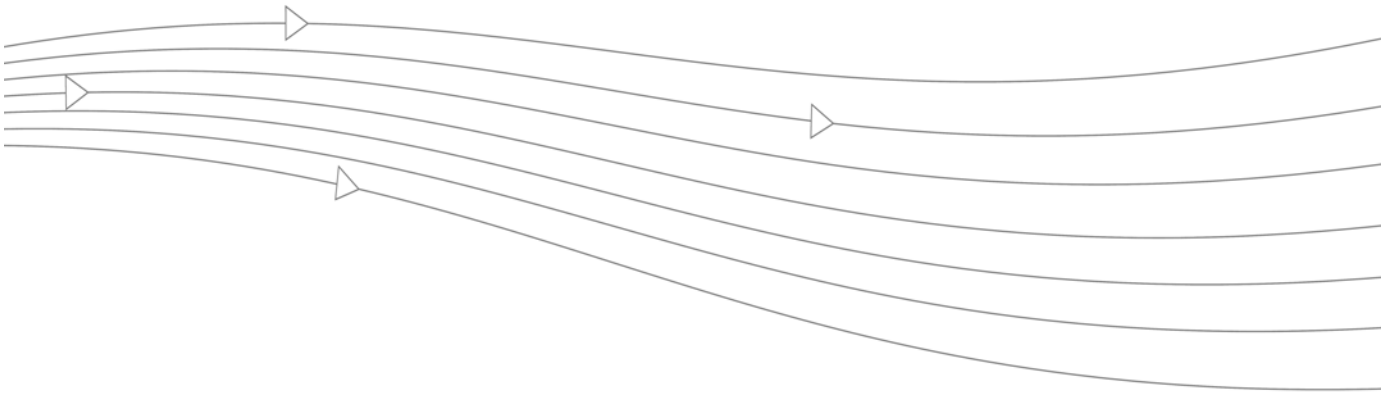
Figure 5 Sequence of Events in Initial Connection



1. X0 interface connects to available segment on gateway. Encrypted session pasees to SSL VPN appliances.
2. The internal networks resource returns content to the SSL VPN appliance through the gateway.
3. SSL VPN traffic traverses the gateway to reach internal network resources.

The SonicWALL SSL-VPN appliances also support “two-arm” deployment scenarios, using one external (DMZ or WAN side) interface and one internal (LAN) interface. However, two-arm mode introduces a lot of routing issues that need to be considered before deployment. SonicWALL does not recommend this type of deployment, because it introduces a number of potential security issues and creates an additional breakpoint in the network since the appliance is essentially a packet filter and is not stateful.

For information about configuring the SonicWALL SSL-VPN to work with third-party gateways, refer to “Configuring SonicWALL SSL VPN with a Third-Party Gateway” on page 271.



Chapter 2: System Configuration

This chapter provides information and configuration tasks specific to the **System** pages on the SonicWALL SSL VPN Web-based management interface, including registering your SonicWALL SSL-VPN appliance, setting the date and time, configuring system settings, system administration and system certificates.

This chapter contains the following sections:

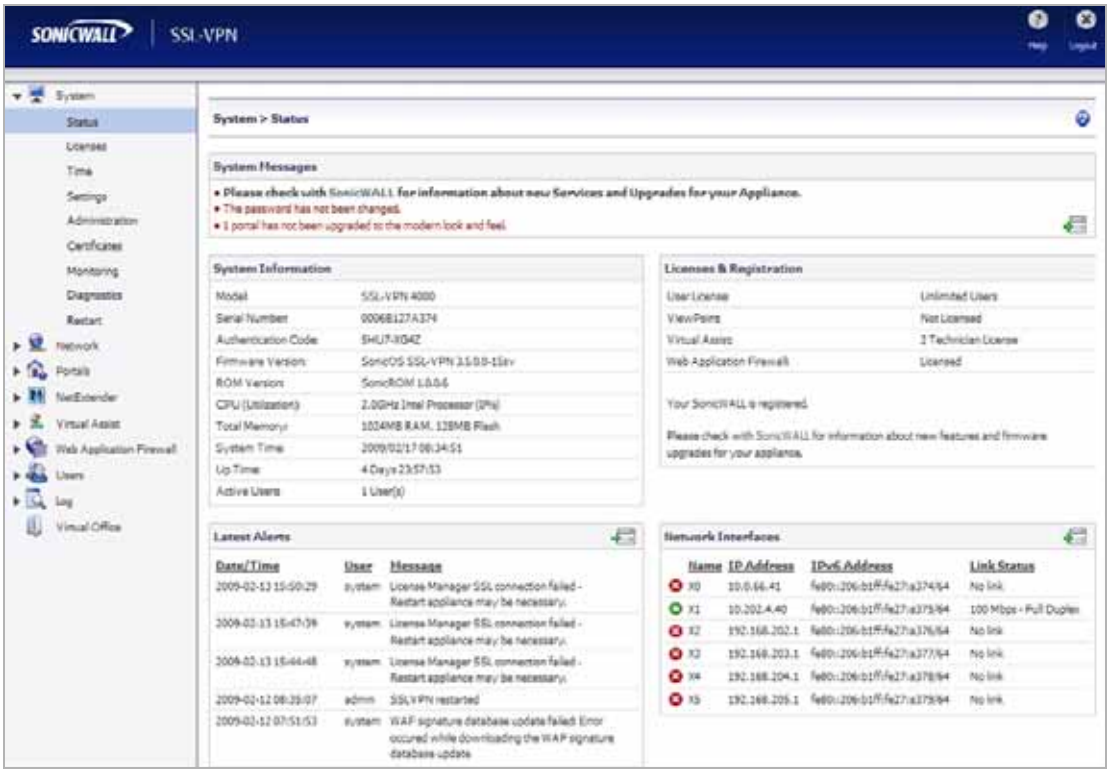
System > Status

This section provides an overview of the **System > Status** page and a description of the configuration tasks available on this page.

System > Status Overview

The **System > Status** page provides the administrator with current system status for the SonicWALL SSL-VPN appliance, including information and links to help manage the SonicWALL SSL-VPN appliance and SonicWALL Security Services licenses. This section provides information about the page display and instructions to perform the configuration tasks on the **System > Status** page.

Figure 6 System > Status Page



Overviews of each area of the **System > Status** page are provided in the following sections:

System Messages

The System Messages section displays text about recent events and important system messages, such as system setting changes. For example, if you do not set an outbound SMTP server, you will see the message, “Log messages and one-time passwords cannot be sent because you have not specified an outbound SMTP server address.”

System Information

The System Information section displays details about your specific SonicWALL SSL-VPN appliance. The following information is displayed in this section:

Table 7 System Information

Field	Description
Model	The type of SonicWALL SSL-VPN appliance.
Serial Number	The serial number or the MAC address of the SonicWALL appliance.
Authentication Code	The alphanumeric code used to authenticate the SonicWALL appliance on the registration database at <https://www.mysonicwall.com>.
Firmware Version	The firmware version loaded on the SonicWALL appliance.
ROM Version	Indicates the ROM version. The ROM code controls low-level functionality of the appliance.
CPU	The type of the SonicWALL appliance processor and the average CPU usage over the last 5 minutes.
System Time	The current date and time.
Up Time	The number of days, hours, minutes, and seconds, that the SonicWALL SSL-VPN appliance has been active since its most recent restart.
Active Users	The number of users who are currently logged into the management interface of the SonicWALL SSL-VPN appliance.

Latest Alerts

The Latest Alerts section displays text about recent invasive events, irregular system behavior, or errors. Latest Alerts includes information about the date and time of the event, the host of the user that generated the event and a brief description of the event.

Any messages relating to system events or errors are displayed in this section. Clicking the arrow button located in upper right corner of this section displays the **Log > Log View** page.

Fields in the Latest Alerts section are:

- **Date/Time** - The date and time when the message was generated.
- **User** - The name of the user that generated the message.
- **Message** - A message describing the error.

Licenses & Registration

The Licenses & Registration section indicates the user license allowance and registration status of your SonicWALL SSL-VPN appliance. The status of your ViewPoint, Virtual Assist, and Web Application Firewall licenses are also displayed here.

To register your appliance on MySonicWALL and manually enter the registration code in the available field at the bottom of this section, see the "Registering Your SonicWALL SSL-VPN from System Status" section on page 62.

To register your appliance on MySonicWALL from the **System > Licenses** page and allow the appliance to automatically synchronize registration and license status with the SonicWALL server, see the "Registering the SSL-VPN from System > Licenses" section on page 67.

Network Interfaces

The Network Interfaces section provides the administrator with a list of SonicWALL SSL-VPN interfaces by name. For each interface, the Network Interfaces tab provides the IP address that has been configured and the current link status.

For information about configuration tasks related to the Network Interfaces section, refer to the "Configuring Network Interfaces" section on page 64.

Registering Your SonicWALL SSL-VPN from System Status

Register with MySonicWALL to get the most out of your SonicWALL SSL-VPN. Complete the steps in the following sections to register.

Before You Register

Verify that the time, DNS, and default route settings on your SonicWALL SSL VPN are correct before you register your appliance. These settings are generally configured during the initial SonicWALL SSL VPN setup process. To verify or configure the time settings, navigate to the **System > Time** page. To verify or configure the DNS setting, navigate to the **Network > DNS** page. To verify or configure the default route, navigate to the **Network > Routes** page. For more information about time and DNS setting configuration, refer to the "Setting the Time" section on page 72, the "Configuring DNS Settings" section on page 95 and the "Configuring a Default Route for the SSL-VPN Appliance" section on page 97.

Note You need a MySonicWALL account to register the SonicWALL SSL VPN.

Registering with MySonicWALL

There are two ways to register your SonicWALL SSL-VPN appliance:

- Log into your MySonicWALL account directly from a browser or click the **SonicWALL** link on the **System > Status** page to access MySonicWALL, enter the appliance serial number and other information there, and then enter the resulting registration code into the field on the **System > Status** page. This manual registration procedure is described in this section.
- Use the link on the **System > Licenses** page to access MySonicWALL, then enter the serial number and other information into MySonicWALL. When finished, your view of the **System > Licenses** page shows that the appliance has been automatically synchronized with the licenses activated on MySonicWALL. This procedure is described in the "Registering the SSL-VPN from System > Licenses" section on page 67.

Step 1 If you are not logged into the SonicWALL SSL VPN management interface, log in with the username ***admin*** and the administrative password you set during initial setup of your SonicWALL SSL-VPN (the default is *password*). For information about configuring the administrative password, refer to the *SonicWALL SSL VPN Getting Started Guide.*

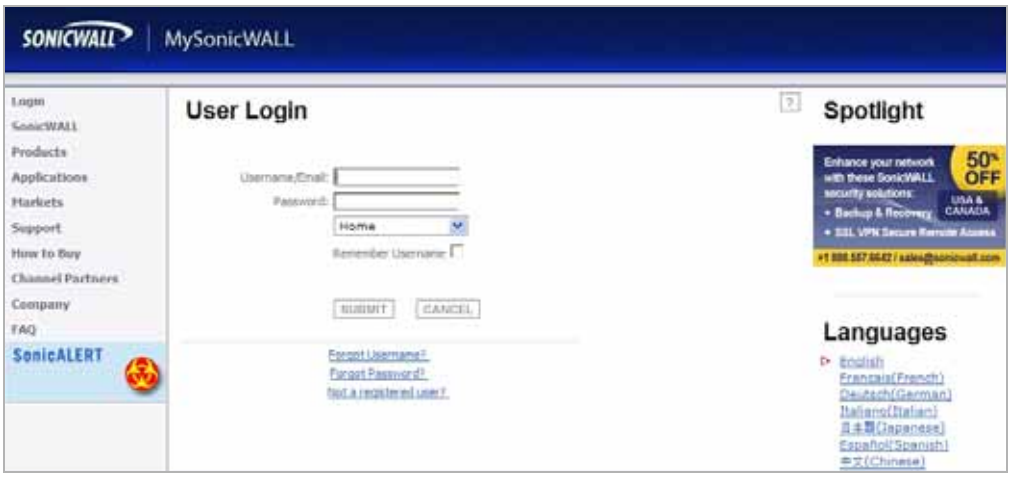
Step 2 If the **System > Status** page is not automatically displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.

Step 3 Record your **Serial Number** and **Authentication Code** from the **Licenses & Registration** section.

Step 4 Do one of the following to access the MySonicWALL Web page:

- Click the **SonicWALL** link in the **Licenses & Registration** section.
- Type http://www.mysonicwall.com into the Address or Location field of your Web browser.

The **MySonicWALL User Login** page is displayed.



Step 5 Enter your MySonicWALL account user name and password.

Note If you are not a registered MySonicWALL user, you must create an account before registering your SonicWALL product. Click the **Not a registered user?** link at the bottom of the page to create your free MySonicWALL account.

Step 6 Navigate to **Products** in the left hand navigation bar.

Step 7 Enter your **Serial Number** and **Authentication Code** in the appropriate fields.

Step 8 Enter a descriptive name for your SonicWALL SSL-VPN in the **Friendly Name** field.

Step 9 Select the product group for this appliance, if any, from the **Product Group** drop-down list.

Step 10 Click the **Register** button.

Step 11 When the MySonicWALL server has finished processing your registration, the Registration Code is displayed along with a statement that your appliance is registered. Click **Continue**.

Step 12 On the **System > Status** page of the SonicWALL SSL VPN management interface, enter the Registration Code into the field at the bottom of the **Licenses & Registration** section, and then click **Update**.

Configuring Network Interfaces

The IP settings and interface settings of the SonicWALL SSL-VPN appliance may be configured by clicking on the blue arrow in the corner of the Network Interfaces section of the **System > Status** page. The link redirects you to the **Network > Interfaces** page, which can also be accessed from the navigation bar. From the **Network > Interfaces** page, a SonicWALL SSL-VPN appliance administrator can configure the IP address of the primary (X0) interface, and also optionally configure additional interfaces for operation.

For a port on your SonicWALL SSL-VPN appliance to communicate with a firewall or target device on the same network, you need to assign an IP address and a subnet mask to the interface.

For more information about configuring interfaces, refer to the “Network > Interfaces” section on page 92.

System > Licenses

This section provides an overview of the **System > Licenses** page and a description of the configuration tasks available on this page. See the following sections:

System > Licenses Overview

Services upgrade licensing and related functionality is provided by the SonicWALL License Manager, which runs on the SonicWALL SSL-VPN appliance. The License Manager communicates periodically (hourly) with the SonicWALL licensing server to verify the validity of licenses. The License Manager also allows the administrator to purchase licenses directly or turn on free trials to preview a product before buying.

Note Initial registration of the unit is required for the License Manager to work.

Licensing is controlled by SonicWALL’s license manager service, and customers can add licenses through their MySonicWALL accounts. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWALL.

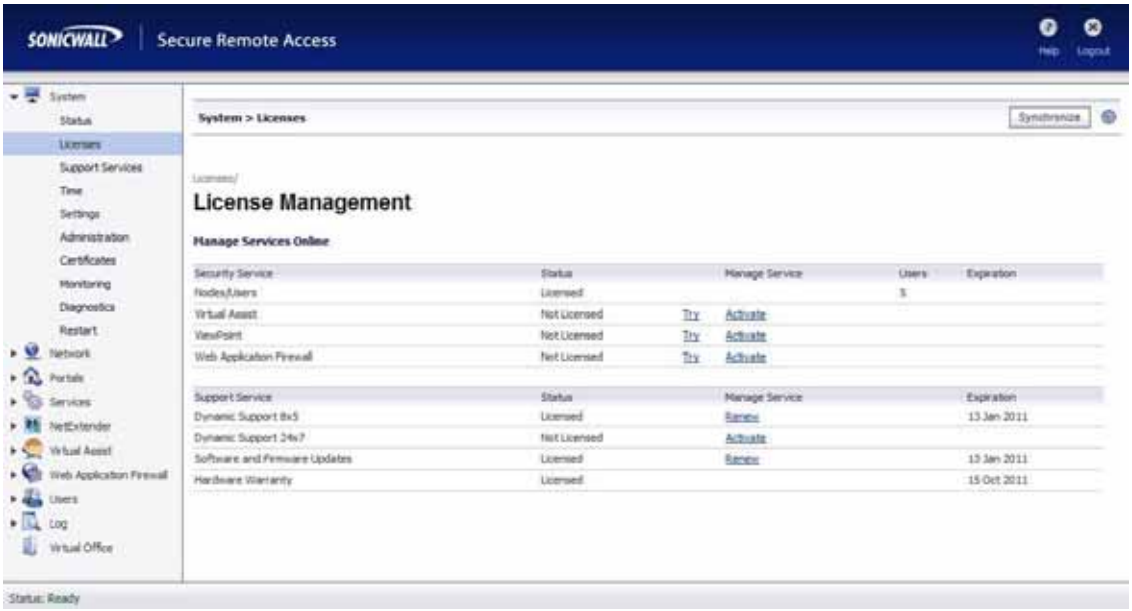
License status is displayed in the SSL VPN management interface, on the Licenses & Registration section of the 'System > Status' page. The TSR, generated on the 'System > Diagnostics' page, displays both the total licenses and active user licenses currently available on the appliance.

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

Note The SonicWALL SSL-VPN 2000 and 4000 appliance models support unrestricted licensing.

The **System > Licenses** page also provides a link to activate, upgrade, or renew SonicWALL Security Services licenses. From this page in the SonicWALL Management Interface, you can manage all the SonicWALL Security Services licenses for your SonicWALL SSL-VPN appliance. The information listed in the Security Services Summary table is updated periodically from your MySonicWALL account.

Figure 7 System > Licenses Page



Security Services Summary

The **Security Services Summary** table lists the number of Nodes/Users licenses and the available and activated security services on the SonicWALL SSL-VPN appliance.

The **Security Service** column lists all the available SonicWALL Security Services and upgrades available for the SonicWALL security appliance. The **Status** column indicates if the security service is activated (Licensed), available for activation (Not Licensed), or no longer active (Expired). ViewPoint and Virtual Assist services are licensed separately as upgrades.

The number of nodes/users allowed by the license is displayed in the **Users** column. A node is a computer or other device connected to your SonicWALL SSL-VPN appliance with an IP address. This number refers to the maximum number of simultaneous connections to the SonicWALL SSL-VPN appliance.

The **Expiration** column displays the expiration date for any licensed service that is time-based.

The information listed in the **Security Services Summary** table is updated from the SonicWALL licensing server every time the SonicWALL SSL-VPN appliance automatically synchronizes with it (hourly), or you can click the **Synchronize** button to synchronize immediately.

Note If the licenses do not update after a synchronize, you may need to restart your SSL-VPN appliance. DNS must be configured properly and the appliance should be able to reach the sonicwall.com domain.

Manage Security Services Online

You can login to MySonicWALL directly from the **System > Licenses** page by clicking the link **Activate, Upgrade, or Renew services**. You can click this link to register your appliance, to purchase additional licenses for upgrading or renewing services, or to activate free trials.

Before You Register

Verify that the time, DNS, and default route settings on your SonicWALL SSL VPN are correct before you register your appliance. These settings are generally configured during the initial SonicWALL SSL VPN setup process. To verify or configure the time settings, navigate to the **System > Time** page. To verify or configure the DNS setting, navigate to the **Network > DNS** page. To verify or configure the default route, navigate to the **Network > Routes** page. For more information about time and DNS setting configuration, refer to the "Setting the Time" section on page 72, the "Configuring DNS Settings" section on page 95 and the "Configuring a Default Route for the SSL-VPN Appliance" section on page 97.

Note You need a MySonicWALL account to register the SonicWALL SSL VPN.

Creating a MySonicWALL Account from System > Licenses

Step 1 On the System > Licenses page, click **Activate, Upgrade, or Renew services**. The License Management page is displayed.

Step 2 If you do not have a MySonicWALL account or if you forgot your user name or password, click the **https://www.mysonicwall.com** link at the bottom of the page. The **MySonicWALL User Login** page is displayed.

Do one of the following:

- If you forgot your user name, click the **Forgot Username?** link.
- If you forgot your password, click the **Forgot Password?** link.
- If you do not have a MySonicWALL account, click the **Not a registered user?** link.

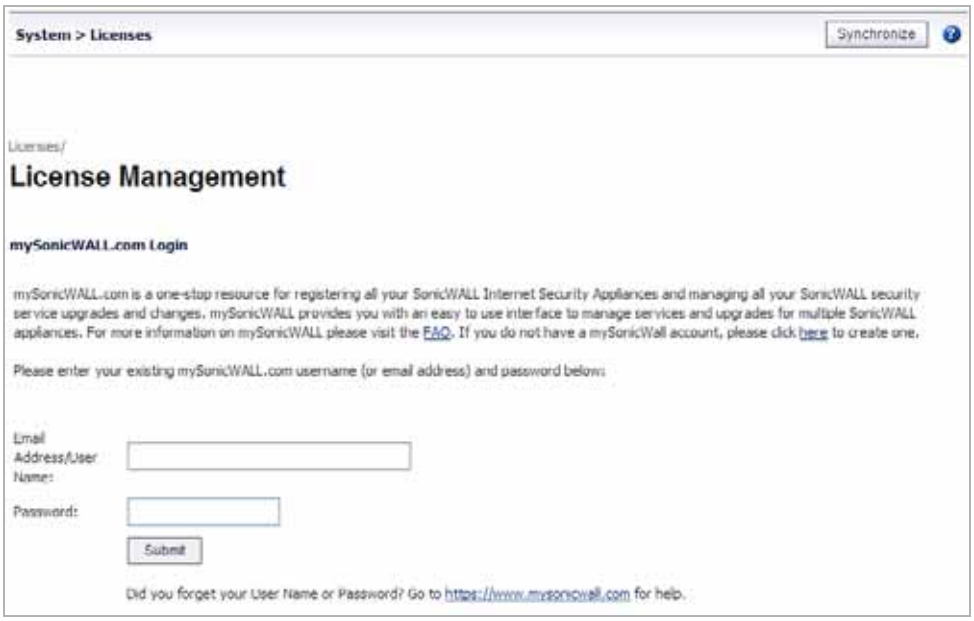
Step 3 Follow the instructions to activate your MySonicWALL account.

Registering the SSL-VPN from System > Licenses

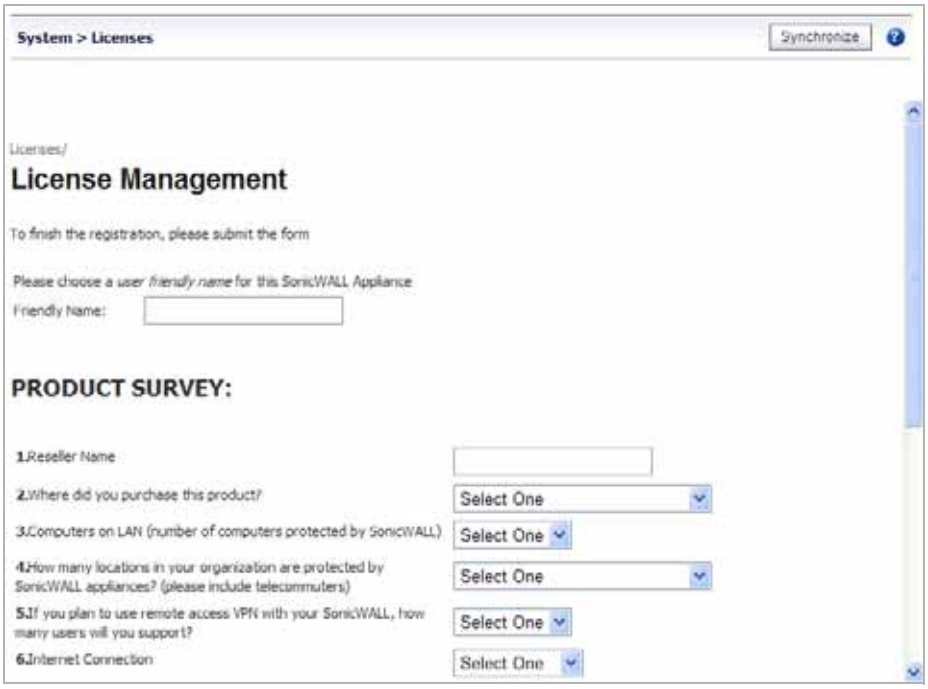
On a new SonicWALL SSL-VPN appliance or after upgrading to SonicWALL SSL VPN 3.0 firmware from an earlier release, you can register your appliance from the **System > Licenses** page.

To register your appliance from the **System > Licenses** page:

Step 1 On the **System > Licenses** page, click **Activate, Upgrade, or Renew services**. The License Management page is displayed.

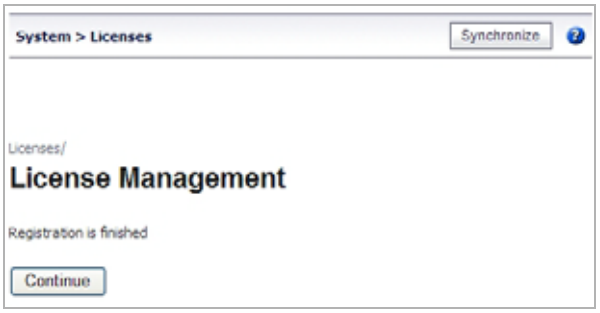


Step 2 Enter your MySonicWALL user name and password into the fields and then click **Submit**. The display changes.



Step 3 Enter a descriptive name for your SonicWALL SSL-VPN in the **Friendly Name** field.

Step 4 Under **Product Survey**, fill in the requested information and then click **Submit**. The display changes to inform you that your SonicWALL SSL VPN is registered.



Step 5 Click **Continue**.

Step 6 In the License Management page, your latest license information is displayed.

Note After registration, some network environments require the SSL-VPN appliance to be offline so that it is unable to connect to the SonicWALL licensing server. In this mode, the appliance will still honor the valid licenses; however, timed-based licenses may not be valid.

Activating or Upgrading Licenses

After your SonicWALL SSL-VPN appliance is registered, you can activate licenses or free trials for Virtual Assist and ViewPoint on the **System > Licenses** page. You can also upgrade a license. For example, if your appliance is licensed for a single Virtual Assist technician, you can upgrade the license for multiple technicians.

You must purchase the license subscription on MySonicWALL or from your reseller before you can activate or upgrade. You will receive an activation key to enter into the License Manager page.

To activate or upgrade licenses or free trials on your appliance:

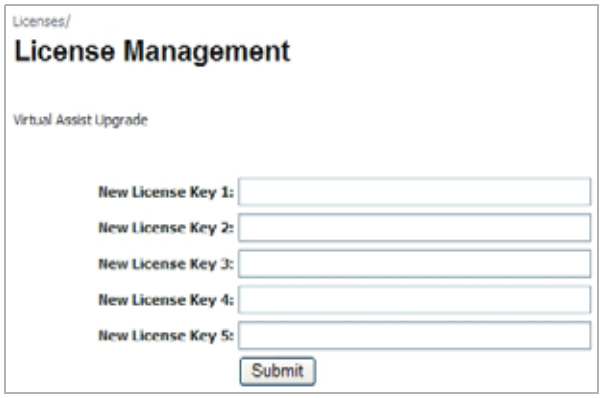
Step 1 On the System > Licenses page, click **Activate, Upgrade, or Renew services**. The License Management page is displayed.

Step 2 Enter your MySonicWALL user name and password into the fields and then click **Submit**. The display changes to show the status of your licenses. Each service can have a **Try** link, an **Activate** link, or an **Upgrade** link.

Step 3 To activate a free 30-day trial, click **Try** next to the service that you want to try. The page explains that you will be guided through the setup of the service, and that you can purchase a SonicWall product subscription at any time during or after the trial. Click **Continue**, and follow the setup instructions.

Step 4 To activate a new license which you have already purchased on MySonicWALL or from your reseller, click **Activate** next to the service that you want to activate. Enter your license activation key into the **<Product> Activation Key** field, and then click **Submit**.

Step 5 To upgrade an existing license with a new license that you have already purchased, click **Upgrade** next to the service that you want to upgrade. Type or paste one or more new activation keys into the **New License Key #** field(s), and then click **Submit**.



Step 6 After completing the activation or upgrading process, click **Synchronize** to update the appliance license status from the SonicWALL licensing server. Rebooting the appliance will also update the license status.

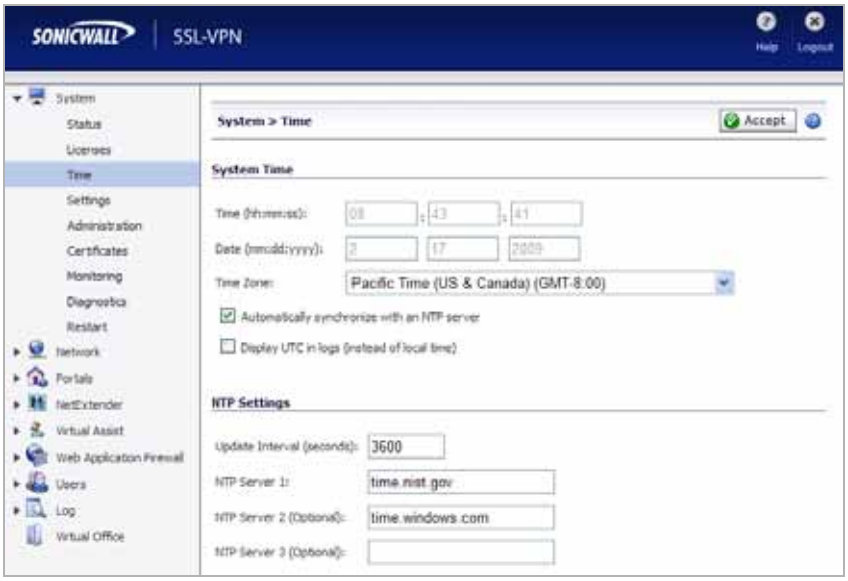
System > Time

This section provides an overview of the **System > Time** page and a description of the configuration tasks available on this page.

System > Time Overview

The **System > Time** page provides the administrator with controls to set the SonicWALL SSL-VPN system time, date and time zone, and to set the SonicWALL SSL-VPN appliance to synchronize with one or more NTP servers.

Figure 8 System > Time Page



System Time

The System Time section allows the administrator to set the time (hh:mm:ss), date (mm:dd:yyyy) and time zone. It also allows the administrator to select automatic synchronization with the NTP (Network Time Protocol) server and to display UTC (Coordinated Universal Time) instead of local time in logs.

NTP Settings

The NTP Settings section allows the administrator to set an update interval (in seconds), an NTP server, and two additional (optional) NTP servers.

Setting the Time

To configure the time and date settings, navigate to the **System > Time** page. The appliance uses the time and date settings to timestamp log events and for other internal purposes. It is imperative that the system time be set accurately for optimal performance and proper registration.

Note For optimal performance, the SonicWALL SSL-VPN appliance must have the correct time and date configured.

To configure the time and date settings, perform the following steps:

Step 1 Select your time zone in the **Time Zone** drop-down list.

Step 2 The current time, in 24-hour time format, will appear in the **Time (hh:mm:ss)** field and the current date will appear in the **Date (mm:dd:yyyy)** field.

Step 3 Alternately, you can manually enter the current time in the **Time (hh:mm:ss)** field and the current date in the **Date (mm:dd:yyyy)** field.

Note If the checkbox next to **Automatically synchronize with an NTP server** is selected, you will not be able to manually enter the time and date. To manually enter the time and date, clear the checkbox.

Step 4 Click **Accept** to update the configuration.

Enabling Network Time Protocol

If you enable Network Time Protocol (NTP), then the NTP time settings will override the manually configured time settings. The NTP time settings will be determined by the NTP server and the time zone that is selected in the **Time Zone** drop-down list.

To set the time and date for the appliance using the Network Time Protocol (NTP), perform the following steps:

Step 1 Navigate to the **System > Time** page.

Step 2 Select the **Automatically synchronize with an NTP server** checkbox.

Step 3 In the NTP Settings section, enter the time interval in seconds to synchronize time settings with the NTP server in the **Update Interval** field. If no period is defined, the appliance will select the default update interval, 64 seconds.

Step 4 Enter the NTP server IP address or fully qualified domain name (FQDN) in the **NTP Server 1** field.

Step 5 For redundancy, enter a backup NTP server address in the **NTP Server Address 2 (Optional)** and **NTP Server Address 3 (Optional)** fields.

Step 6 Click **Accept** to update the configuration.

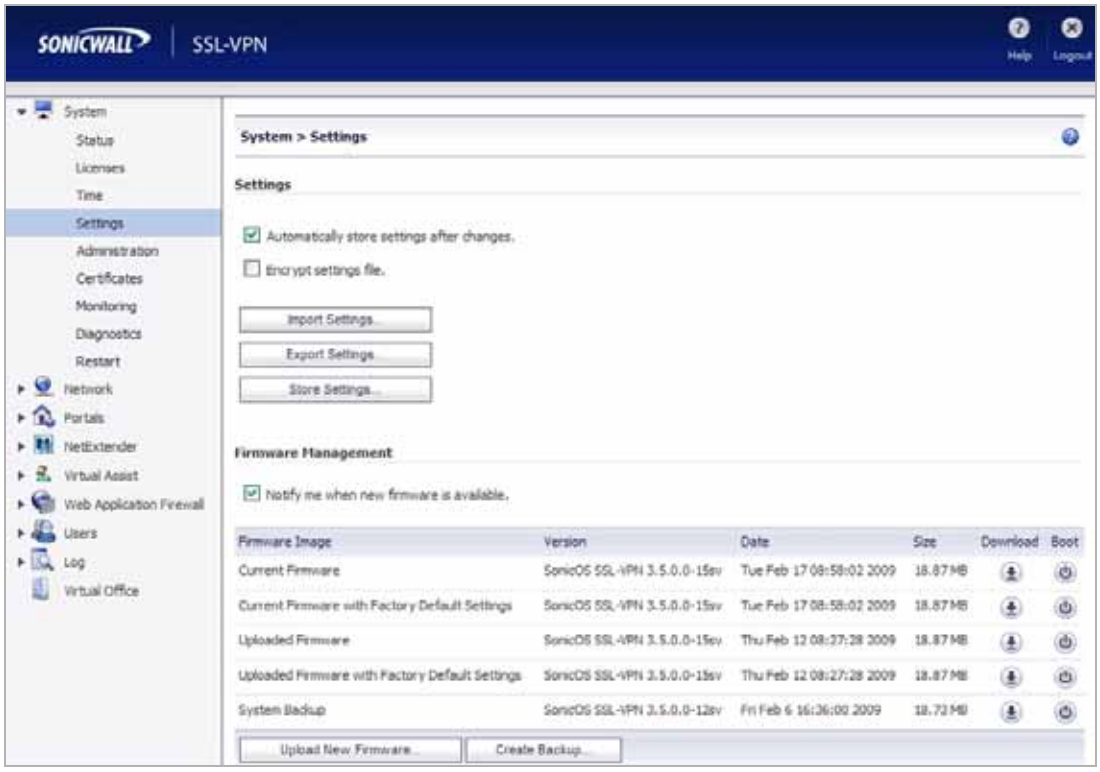
System > Settings

This section provides an overview of the **System > Settings** page and a description of the configuration tasks available on this page.

System > Settings Overview

The **System** > **Settings** page allows the administrator to manage the firmware and related settings of the SonicWALL SSL-VPN appliance:

Figure 9 System > Settings Page



Settings

The Settings section allows the administrator to automatically store settings after changes and to encrypt the settings file. This section also provides buttons to import settings, export settings, and store settings.

Firmware Management

The Firmware Management section allows the administrator to control the firmware that is running on the SSL-VPN appliance. This section provides buttons for uploading new firmware, creating a backup of current firmware, downloading existing firmware to the management computer, rebooting the appliance with current or recently uploaded firmware, and rebooting the appliance with factory default settings. There is also an option to be notified when new firmware becomes available.

Managing Configuration Files

SonicWALL allows you to save and import file sets that hold the SSL VPN configuration settings. These file sets can be saved and uploaded through the **System > Settings** page in the SSL VPN management interface.

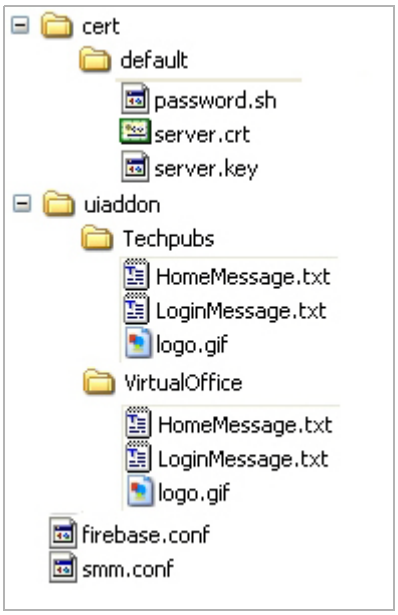
These tasks are described in the following sections:

- "Exporting a Backup Configuration File" section on page 74
- "Importing a Configuration File" section on page 75
- "Storing Settings" section on page 76
- "Automatically Storing Settings After Changes" section on page 76
- "Encrypting the Configuration File" section on page 76

Exporting a Backup Configuration File

Exporting a backup configuration file allows you to save a copy of your configuration settings on your local machine. You may then save the configuration settings or export them to a backup file and import the saved configuration file at a later time, if necessary. The backup file is called **sslvpnSettings-serialnumber.zip** by default, and includes the contents in Figure 10.

Figure 10 Backup Configuration Directory Structure in Zip File



The backup directory structure contains the following elements:

- **ca** folder (not shown) – Contains CA certificates provided by a Certificate Authority.
- **cert** folder – Contains the **default** folder with the default key/certification pair. Also contains key/certification pairs generated by Certificate Signing Requests (CSRs) from the **System > Certificates** page, if any.
- **uiaddon** folder – Contains a folder for each portal. Each folder contains portal login messages, portal home page messages, and the default logo or the custom logo for that portal, if one was uploaded. **VirtualOffice** is the default portal.
- **firebase**.**conf** file – Contains network, DNS and log settings.
- **smm**.**conf** file – Contains user, group, domain and portal settings.

To export a backup configuration file, perform the following steps:

Step 1 Navigate to the **System > Settings** page.

Step 2 To save a backup version of the configuration, click **Export Settings**. The browser you are working in displays a pop-up asking you if you want to open the configuration file.

Step 3 Select the option to **Save** the file.

Step 4 Choose the location to save the configuration file. The file is named **sslvpnSettings-serialnumber.zip** by default, but it can be renamed.

Step 5 Click **Save** to save the configuration file.

Importing a Configuration File

You may import the configuration settings that you previously exported to a backup configuration file. To import a configuration file, perform the following steps:

Step 1 Navigate to the **System > Settings** page.

Step 2 To import a backup version of the configuration, click **Import Settings**. The **Import Settings** dialog box is displayed.

Step 3 Click **Browse** to navigate to a location that contains the file (that includes settings) you want to import. The file can be any name, but is named **sslvpnSettings-serialnumber.zip** by default.

Step 4 Click **Upload**. SonicOS SSL VPN imports the settings from the file and configures the appliance with those settings.

Note Make sure you are ready to reconfigure your system. Once you import the file, the system overwrites the existing settings immediately.

Step 5 Once the file has been imported, restart the appliance to make the changes permanent.

Storing Settings

To store settings you created in your recent configuration session, click the **Store Settings** button under the Settings section in the **System > Settings** page.

Automatically Storing Settings After Changes

The **System > Settings** page provides a way to save the current configuration to flash memory.

To automatically store settings after changes, select the **Automatically store settings after changes** checkbox. The system will automatically store configuration to a file in flash memory so that if is rebooted, the latest configuration will be reloaded. If you do not enable this checkbox, the system will prompt you to save settings every time you attempt to reboot the SonicWALL SSL-VPN appliance.

Encrypting the Configuration File

For security purposes, you can encrypt the configuration files in the **System > Settings** page. However, if the configuration files are encrypted, they cannot be edited or reviewed for troubleshooting purposes.

To encrypt the configuration files, select the **Encrypt settings file** checkbox in the **System > Settings** page.

Managing Firmware

The Firmware Management section of **System > Settings** provides the administrator with the option to be notified when new firmware becomes available. It provides the configuration options for firmware images, including uploading new firmware and creating a backup.

These tasks are described in the following sections:

- "Setting Firmware Notification" section on page 76
- "Downloading Firmware" section on page 76
- "Booting a Firmware Image" section on page 77
- "Uploading New Firmware" section on page 77
- "Creating a Backup" section on page 77

Setting Firmware Notification

The administrator can be notified by email when a new firmware build is available.

To be notified when new firmware is available, select the **Notify me when new firmware is available** checkbox.

Downloading Firmware

To download firmware, click the download icon  next to the Firmware Image version you want to download.

Booting a Firmware Image

To boot a firmware image, perform the following steps:

Step 1 Click the boot icon  next to the Firmware Image version that you want to run on the SonicWALL SSL-VPN appliance.

Step 2 The pop-up message is displayed: **Are you sure you wish to boot this firmware?** Click **OK**.

Uploading New Firmware

To upload new firmware, perform the following steps:

Step 1 Login to MySonicWALL.

Step 2 Download the latest SonicWALL SSL VPN firmware version.

Step 3 In the SonicWALL SSL VPN management interface, navigate to **System > Settings** page.

Step 4 Click the **Upload New Firmware** button under the Firmware Management section.

Step 5 Click **Browse**.

Step 6 Select the downloaded SonicWALL SSL VPN firmware. It should have a .sig file extension.

Step 7 Click **Open**.

Step 8 Click **Upload**.

Step 9 The SonicWALL SSL-VPN appliance will automatically reboot when the new firmware has been uploaded.

Creating a Backup

To create a system backup of the current firmware and settings, click the **Create Backup** button. The backup may take up to two minutes. When the backup is complete, the **Status** at the bottom of the screen will display the message “System Backup Successful.”

Note The **Create Backup** button is only available on the SonicWALL SSL-VPN 2000 and 4000.

System > Administration

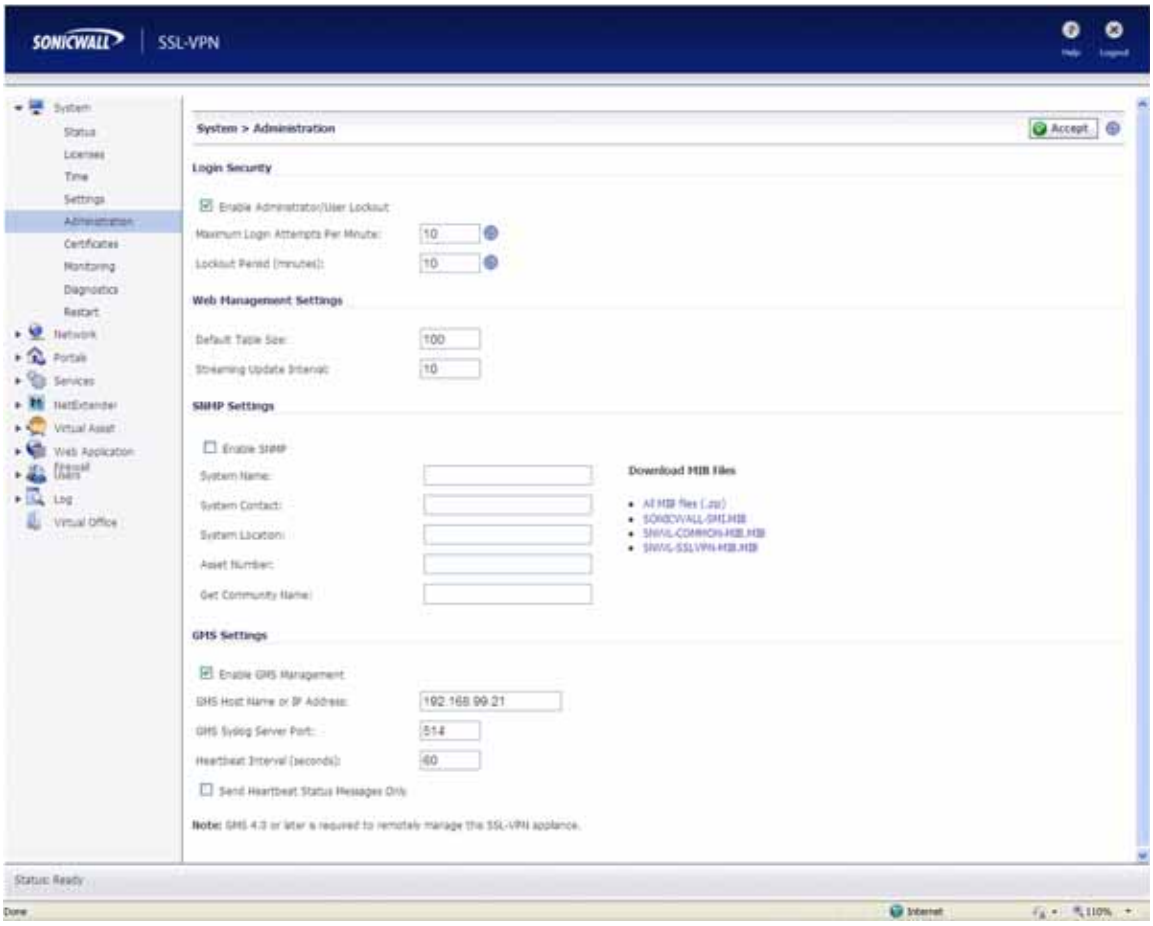
This section provides an overview of the **System > Administration** page and a description of the configuration tasks available on this page.

System > Administration Overview

This section provides the administrator with information about and instructions to perform the configuration tasks on the **System > Administration** page. The **System > Administration** page allows the administrator to configure login security, GMS settings, and to select the interface language.

See the following sections:

Figure 11 System > Administration Page



Login Security

The Login Security section provides a way to configure administrator/user lockout for a set period of time (in minutes) after a set number of maximum login attempts per minute.

GMS Settings

The GMS Settings section allows the administrator to enable GMS management, and specify the GMS host name or IP address, GMS Syslog server port and heartbeat interval (in seconds).

Note GMS 4.0 (or higher) is required to remotely manage SSL-VPN appliances.

Web Management Settings

The Web Management Settings section allows the administrator to set the default page size for paged tables and the streaming update interval for dynamically updated tables in the management interface.

The following paged tables are affected by the Default Table Size setting:

- Virtual Assist > Log
- Web Application Firewall > Log
- Log > View

The minimum for the Default Table Size field is 10 rows, the default is 100, and the maximum is 99,999.

The following dynamically updated tables are affected by the Streaming Update Interval setting:

- System > Monitoring
- Network > Interfaces
- NetExtender > Status
- Users > Status

The minimum for the Streaming Update Interval field is 1 second, the default is 10 seconds, and the maximum is 99,999.

Configuring Login Security

SonicWALL SSL VPN login security provides an auto lockout feature to protect against unauthorized login attempts on the user portal. Complete the following steps to enable the auto lockout feature:

Step 1 Navigate to **System > Administration**.

Step 2 Select the **Enable Administrator/User Lockout** checkbox.

Step 3 In the **Maximum Login Attempts Per Minute** field, type the number of maximum login attempts allowed before a user will be locked out. The default is 5 attempts. The maximum is 99 attempts.

Step 4 In the **Lockout Period (minutes)** field, type a number of minutes to lockout a user that has exceeded the number of maximum login attempts. The default is 55 minutes. The maximum is 9999 minutes.

Step 5 Click the **Accept** button to save your changes.

Enabling GMS Management

The SonicWALL Global Management System (SonicWALL GMS) is a Web-based application that can configure and manage thousands of SonicWALL Internet security appliances, including global administration of multiple site-to-site VPNs from a central location.

Complete the following steps to enable SonicWALL GMS management of your SonicWALL SSL-VPN appliance:

Step 1 Navigate to **System > Administration**.

Step 2 Select the **Enable GMS Management** checkbox.

Step 3 Type the host name or IP address of your GMS server in the **GMS Host Name or IP Address** field.

Step 4 Type the port number of your GMS server in the **GMS Syslog Server Port** field. The default for communication with a GMS server is port 514.

Step 5 Type the desired interval for sending heartbeats to the GMS server in the **Heartbeat Interval (seconds)** field. The maximum heartbeat interval is 86400 seconds (24 hours).

Step 6 Click the **Accept** button to save your changes.

Configuring Web Management Settings

The Web Management Settings section allows the administrator to set the default page size for paged tables and the streaming update interval for dynamically updated tables in the management interface.

To set the table page size and streaming update interval, perform the following steps:

Step 1 In the **Default Table Size** field, enter the number of rows per page for paged tables in the management interface. The default is 100, the minimum is 10, and the maximum is 99,999.

Step 2 In the **Streaming Update Interval** field, enter the number of seconds between updates for dynamically updated tables in the management interface. The default is 10, the minimum is 1, and the maximum is 99,999.

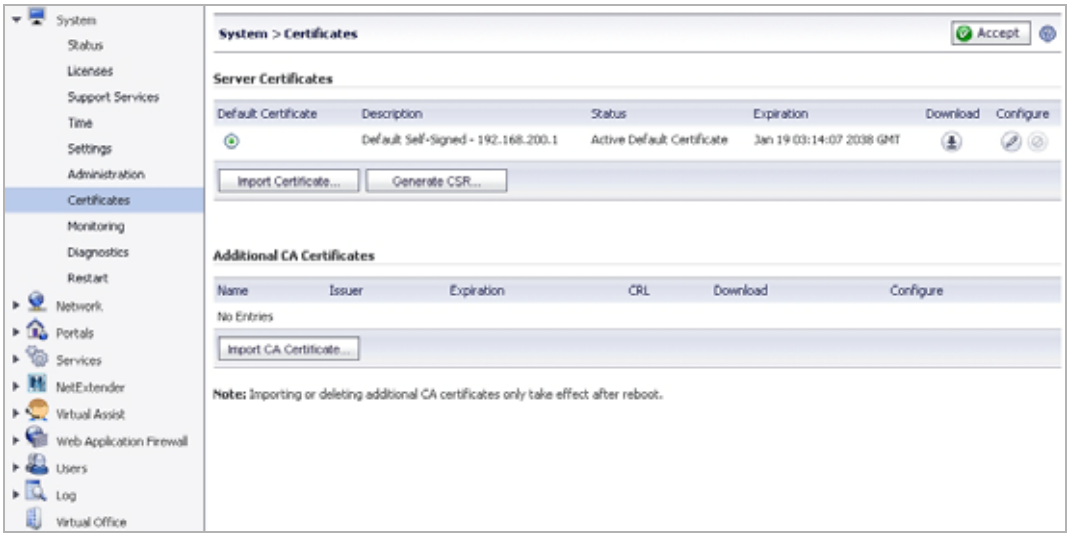
System > Certificates

This section provides an overview of the **System > Certificates** page and a description of the configuration tasks available on this page.

System > Certificates Overview

The **System > Certificates** page allows the administrator to import server certificates and additional CA (Certificate Authority) certificates.

Figure 12 System > Certificates Page



Server Certificates

The Server Certificates section allows the administrator to import and configure a server certificate, and to generate a CSR (certificate signing request).

A server certificate is used to verify the identity of the SonicWALL SSL-VPN appliance. The SSL-VPN presents its server certificate to the user's browser when the user accesses the login page. Each server certificate contains the name of the server to which it belongs.

There is always one self-signed certificate (self-signed means that it is generated by the SonicWALL SSL-VPN appliance, not by a real CA), and there may be multiple certificates imported by the administrator. If the administrator has configured multiple portals, it is possible to associate a different certificate with each portal. For example, **sslvpn.test.sonicwall.com** might also be reached by pointing the browser to **virtualassist.test.sonicwall.com**. Each of those portal names can have its own certificate. This is useful to prevent the browser from displaying a certificate mismatch warning, such as "This server is abc, but the certificate is xyz, are you sure you want to continue?".

A CSR is a certificate signing request. When preparing to get a certificate from a CA, you first generate a CSR with the details of the certificate. Then the CSR is sent to the CA with any required fees, and the CA sends back a valid signed certificate.

Additional CA Certificates

The Additional CA Certificates section allows the administrator to import additional certificates from a Certificate Authority server, either inside or outside of the local network. The certificates are in PEM encoded format for use with chained certificates, for example, when the issuing CA uses an intermediate (chained) signing certificate.

The imported additional certificates only take effect after restarting the SonicWALL SSL-VPN appliance.

Certificate Management

The SonicWALL SSL-VPN comes with a pre-installed self-signed X509 certificate for SSL functions. A self-signed certificate provides all the same functions as a certificate obtained through a well-known certificate authority (CA), but will present an “untrusted root CA certificate” security warning to users until the self-signed certificate is imported into their trusted root store. This import procedure can be performed by the user by clicking the **Import Certificate** button within the portal after authenticating.

The alternative to using the self-signed certificate is to generate a certificate signing request (CSR) and to submit it to a well-known CA for valid certificate issuance. Well-known CAs include RapidSSL (www.rapidssl.com), Verisign (www.verisign.com), and Thawte (www.thawte.com).

Generating a Certificate Signing Request

In order to get a valid certificate from a widely accepted CA such as RapidSSL, Verisign, or Thawte, you must generate a Certificate Signing Request (CSR) for your SonicWALL SSL-VPN appliance. To generate a certificate signing request, perform the following steps:

Step 1 Navigate to the **System > Certificates** page.

Step 2 Click **Generate CSR** to generate a CSR and Certificate Key. The **Generate Certificate Signing Request** dialog box is displayed.

Step 3 Fill in the fields in the dialog box and click **Submit**.

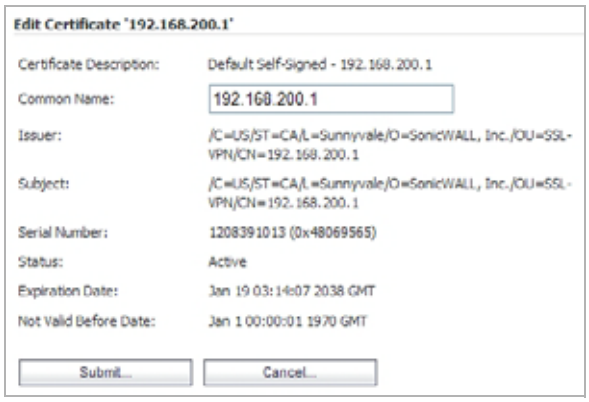
Step 4 If all information is entered correctly, a **csr.zip** file will be created. Save this .zip file to disk. You will need to provide the contents of the server.crt file, found within this zip file, to the CA.

Viewing Certificate and Issuer Information

The Current Certificates table in **System > Certificates** lists the currently loaded SSL certificates.

To view certificate and issuer information, perform the following steps:

Step 1 Click the configure icon for the certificate. The **Edit Certificate** dialog box is displayed, showing issuer and certificate subject information.



Step 2 From the **Edit Certificate** dialog box, you may view the issuer and certificate subject information.

Step 3 Update the certificate common name by entering the correct IP address or string in the **Common Name** field.

Step 4 Click **Submit** to submit the changes.

You may also delete an expired or incorrect certificate. Delete the certificate by clicking the **Delete** button in the row for the certificate, on the System > Certificates page.

Note A certificate that is currently active cannot be deleted. To delete a certificate, upload and enable another SSL certificate, then delete the inactive certificate on the **System > Certificates** page.

Importing a Certificate

When importing a certificate you must upload either a **PKCS #12** (.p12 or.pfx) file containing the private key and certificate, or a zip file containing the PEM-formatted private key file named “server.key” and the PEM-formatted certificate file named **server.crt**. The .zip file must have a flat file structure (no directories) and contain only **server.key** and **server.crt** files.

To import a certificate, perform the following steps:

Step 1 Navigate to the **System** > **Certificates** page.

Step 2 Click **Import Certificate**. The Import Certificate dialog box is displayed.

Step 3 Click **Browse**.

Step 4 Locate the zipped file that contains the private key and certificate on your disk or network drive and select it. Any filename will be accepted, but it must have the ".zip" extension. The zipped file should contain a certificate file named **server.crt** and a certificate key file named **server.key**. The key and certificate must be at the root of the zip, or the file will not be uploaded.

Step 5 Click **Upload**.

Once the certificate has been uploaded, the certificate will be displayed in the Certificates list in the **System > Certificates** page.

Note Private keys may require a password.

Adding Additional CA Certificates

You can import additional CA certificates for use with chained certificates, for example, when the issuing CA uses an intermediate (chained) signing certificate. To import a CA certificate file, upload a **PEM-encoded**, **DER-encoded**, or **PKCS #7** (.p7b) file.

To add additional certificates in PEM format, perform the following steps:

Step 1 Navigate to the **System > Certificates** page.

Step 2 Click **Import CA Certificate** in the Additional CA Certificates section. The Import Certificate dialog box is displayed.

Step 3 Click **Browse**.

Step 4 Locate the PEM-encoded, DER-encoded, or PKCS #7 CA certificate file on your disk or network drive and select it. Any filename will be accepted.

Step 5 Click **Upload**.

Once the certificate has been uploaded, the CA certificate will be displayed in the Additional CA Certificates list in the **System > Certificates** page.

Step 6 To add the new CA certificate to the Web server's active CA certificate list, the Web server must be restarted. Restart the SonicWALL SSL-VPN appliance to restart the Web server.

System > Monitoring

This section provides an overview of the **System > Monitoring** page and a description of the configuration tasks available on this page.

- "System > Monitoring Overview" section on page 85
- "Setting The Monitoring Period" section on page 86
- "Refreshing the Monitors" section on page 86

System > Monitoring Overview

The SonicWALL SSL-VPN appliance provides configurable monitoring tools that enable you to view usage and capacity data for your appliance. The **System > Monitoring** page provides the administrator with four monitoring graphs:

- Active Concurrent Users
- Bandwidth Usage
- CPU Utilization (%)
- Memory Utilization (%)

The administrator can configure the following monitoring periods: last 30 seconds, last 30 minutes, last 24 hours, last 30 days. For example, **Last 24 Hours** refers to the most recent 24 hour period.

Figure 13 System > Monitoring Page

Monitoring Graphs

The four monitoring graphs can be configured to display their respective data over a period of time ranging from the last hour to the last month.

Table 8 Monitoring Graph Types.

Graph	Description
Active Concurrent Users	The number of users who are logged into the appliance at the same time, measured over time by seconds, minutes, hours, or days. This figure is expressed as an integer, for example, 2, 3, or 5.
Bandwidth Usage (Kbps)	Indicates the amount of data per second being transmitted and received by the appliance in Kbps measured over time by seconds, minutes, hours, or days.
CPU Utilization (%)	The amount of capacity usage on the appliance processor being used, measured over time by seconds, minutes, hours, or days. This figure is expressed as a percentage of the total capacity on the CPU.
Memory Utilization (%)	The amount of memory available used by the appliance, measured over time by seconds, minutes, hours, or days. This monitoring graph displays memory utilization as a percentage of the total memory available.

Setting The Monitoring Period

To set the monitoring period, select one of the following options from the **Monitor Period** drop-down list in the **System > Monitoring** page:

- Last 30 Seconds
- Last 30 Minutes
- Last 24 Hours
- Last 30 Days

Refreshing the Monitors

To refresh the monitors, click the **Refresh** button at the top right corner of the **System > Monitoring** page.

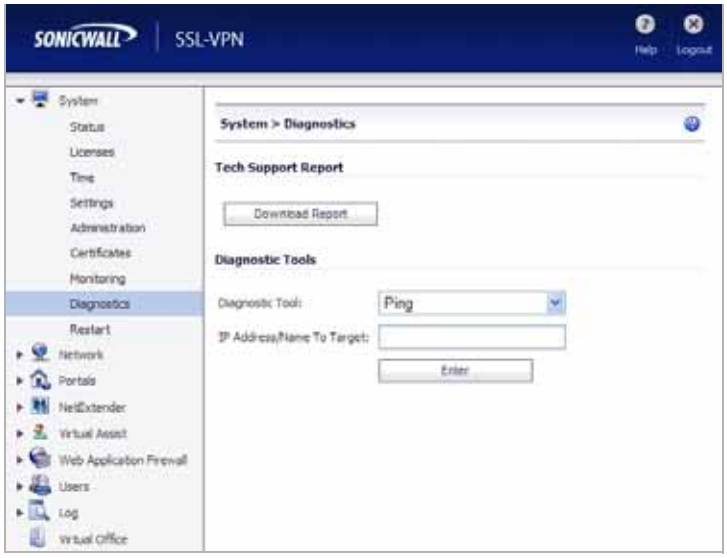
System > Diagnostics

This section provides an overview of the **System > Diagnostics** page and a description of the configuration tasks available on this page.

System > Diagnostics Overview

The **System > Diagnostics** page allows the administrator to download a tech support report and perform basic network diagnostics.

Figure 14 System > Diagnostics Page



Tech Support Report

Downloading a Tech Support Report records system information and settings that are useful to SonicWALL Technical Support when analyzing system behavior. To download the Tech Support report, click **Download Report** under Tech Support Report. For information about configuration tasks related to the Tech Support Report section, refer to the "Downloading the Tech Support Report" section on page 88.

Diagnostic Tools

Diagnostic tools allows the administrator to test SSL-VPN connectivity by performing a ping, DNS lookup, or Traceroute for a specific IP address or Web site. For information about configuration tasks related to the Diagnostic Tools section, refer to "Performing Diagnostic Tests" section on page 88.

Downloading the Tech Support Report

To download the tech support report, click the **Download Report** button on the **System > Diagnostics** page. A Windows pop-up will display confirming the download. Click **Save** to save the report. The tech support report is saved as a .zip file, containing graphs, event logs and other technical information about your SSL-VPN.

Performing Diagnostic Tests

You can perform standard network diagnostic tests on the SonicWALL SSL-VPN appliance in the **System > Diagnostics** page. To run a diagnostic test, perform the following steps:

Step 1 Navigate to the **System** > **Diagnostics** page.

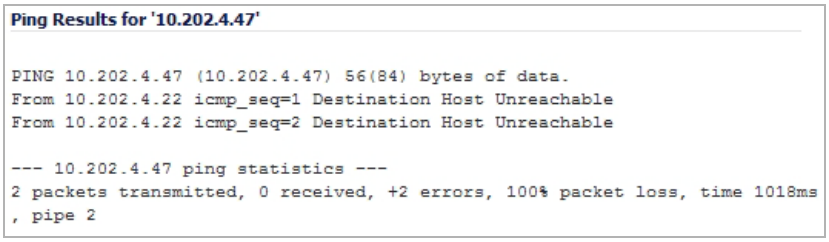
Step 2 In the **Diagnostic Tool** drop-down list, select **Ping**, **DNS Lookup**, **Traceroute**, **Ping6**, **Traceroute6**.

Ping6 and **Traceroute6** are meant for use with IPv6 addresses and networks.

Step 3 In the **IP Address/Name to Target** field, type an IP address or domain name you wish to attempt to reach. Type an IPv6 address or domain if using **Ping6** or **Traceroute6**.

Step 4 Click **Enter**.

Step 5 The results display at the bottom of the page.



System > Restart

This section provides an overview of the **System > Restart** page and a description of the configuration tasks available on this page.

System > Restart Overview

The **System > Restart** page allows the administrator to restart the SonicWALL SSL-VPN appliance.

Figure 15 System > Restart Page

Restarting the SonicWALL SSL-VPN

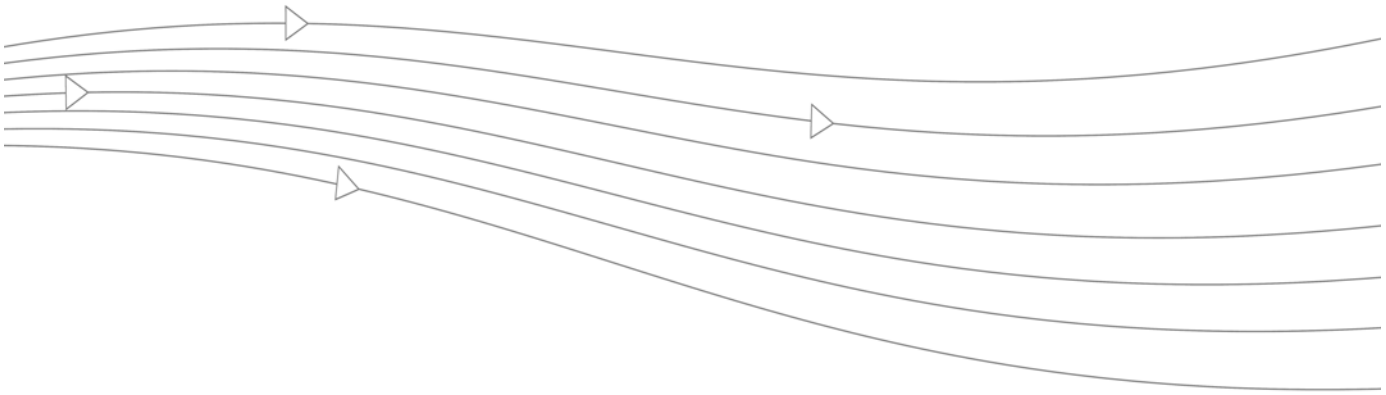
To restart the SSL-VPN appliance:

Step 1 Navigate to **System > Restart**.

Step 2 Click the **Restart** button.

Step 3 In the confirmation dialog box, click **OK**.

Note Restarting takes approximately 2 minutes and causes all users to be disconnected.



Chapter 3: Network Configuration

This chapter provides information and configuration tasks specific to the **Network** pages on the SonicWALL SSL VPN Web-based management interface. Network tasks for the SonicWALL SSL-VPN appliance include configuring network interfaces, DNS settings, routes, and host resolution.

This chapter contains the following sections:

Network > Interfaces

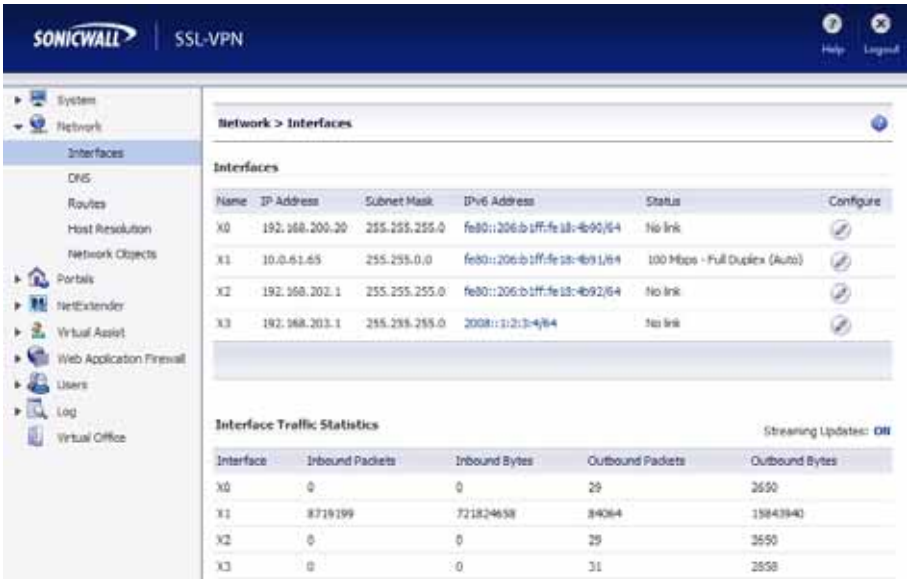
This section provides an overview of the **Network > Interfaces** page and a description of the configuration tasks available on this page.

Network > Interfaces Overview

The **Network > Interfaces** page allows the administrator to configure the IP address, subnet mask and view the connection speed of physical network interface ports on the SonicWALL SSL-VPN appliance.

Note IPv6 addresses are supported only on SonicWALL SSL-VPN models 2000 or higher.

Figure 16 SSL-VPN models 2000 or higher Network > Interfaces Page



Configuring Network Interfaces

The **Network > Interfaces** page allows the administrator to view and configure the IP address, subnet mask, speed, and management settings of the X0, X1, X2, X3, and where available, the X4 and X5 interfaces on the SonicWALL SSL-VPN appliance. For a port on your SonicWALL SSL-VPN appliance to communicate with a firewall or target device on the same network, you need to assign an IP address and a subnet mask to the interface.

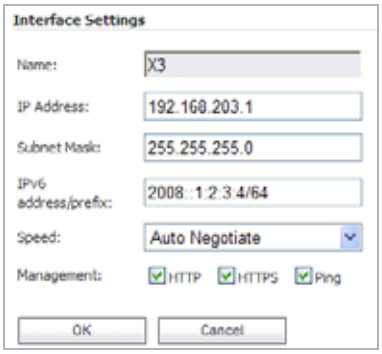
Note If the management interface IP address changes, the SonicWALL SSL VPN services will be automatically restarted. This interrupts any existing user sessions, and users will need to reconnect to continue using the SonicWALL SSL-VPN.

To configure these settings for an interface on the SonicWALL SSL-VPN appliance, perform the following steps:

Step 1 Navigate to the **Network > Interfaces** page and click the configure icon next to the interface you want to configure.

Step 2 In the **Edit Interfaces** dialog box on the SonicWALL SSL-VPN appliance, type an unused static IP address in the **IP Address** field. This IP address should reside within the local subnet to which your SonicWALL SSL-VPN appliance is connected.

Step 3 Type **Subnet Mask** in the corresponding field.



Step 4 On SonicWALL SSL-VPN models 2000 and higher, in the **IPv6 address/prefix** field, optionally enter an IPv6 address for global scope. If you leave this field empty, IPv6-enabled devices can still automatically connect using a link-local address. The scope is indicated in a tooltip on the Network > Interfaces page.

Step 5 In the **Speed** drop-down list, **Auto Negotiate** is selected by default to allow the SSL-VPN appliance to automatically negotiate the speed and duplex mode with the connected switch or other networking device. Ethernet connections are typically auto-negotiated. If you want to force a certain link speed and duplex mode, select one of the following options:

- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

Note If you select a specific link speed and duplex mode, you must force the connection speed and duplex from the connected networking device to the SonicWALL security appliance as well.

Step 6 For the **Management** options, if you want to enable remote management of the SonicWALL SSL-VPN appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, and/or **Ping**.

Step 7 Click **OK**.

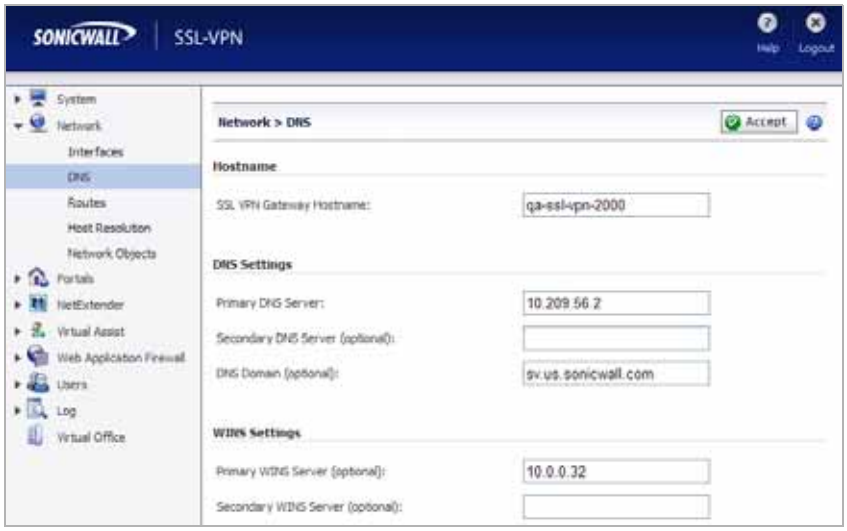
Network > DNS

This section provides an overview of the **Network > DNS** page and a description of the configuration tasks available on this page.

Network > DNS Overview

The **Network > DNS** page allows the administrator to set the SonicWALL SSL-VPN appliance hostname, DNS settings and WINS settings.

Figure 17 SSL-VPN models 2000 or higher Network > DNS Page



Hostname

The hostname section allows the administrator to specify the SSL VPN gateway hostname.

DNS Settings

The DNS settings section allows the administrator to specify a primary DNS server, secondary (optional) DNS server and DNS domain (optional). The primary DNS server is required.

WINS Settings

The WINS (Windows Internet Name Server) settings section allows the administrator to specify the primary WINS server and secondary WINS server (both optional).

Configuring Hostname Settings

To configure a hostname, perform the following steps:

Step 1 Navigate to the **Network > DNS** page.

Step 2 In the Hostname region, type a hostname for the SonicWALL SSL-VPN appliance in the **SSL VPN Gateway Hostname** field.

Step 3 Click **Accept**.

Configuring DNS Settings

The Domain Name Server (DNS) is required to allow your SonicWALL SSL-VPN appliance to resolve host names and URL names with a corresponding IP address. This enables your SonicWALL SSL-VPN appliance to connect to hosts or sites using a Fully Qualified Domain Name (FQDN).

To configure the DNS server, perform the following steps:

Step 1 Navigate to the **Network > DNS** page.

Step 2 In the DNS Settings region, type the address of the primary DNS server in the **Primary DNS Server** field.

Step 3 An optional secondary address can be provided in the **Secondary DNS Server (optional)** field.

Step 4 An optional DNS domain suffix can be provided in the **DNS Domain (optional)** field.

Step 5 Click **Accept**.

Configuring WINS Settings

WINS settings are optional. The SonicWALL SSL-VPN appliance can act as both a NetBIOS and WINS (Windows Internet Naming Service) client to learn local network host names and corresponding IP addresses.

To configure WINS settings, perform the following tasks:

Step 1 Navigate to the **Network > DNS** page.

Step 2 In the WINS Settings region, type a primary WINS address in the **Primary WINS Server (optional) field**.

Step 3 In the WINS settings region, type a secondary WINS address in the **Secondary WINS Server (optional)** field.

Step 4 Click **Accept**.

Network > Routes

This section provides an overview of the **Network > Routes** page and a description of the configuration tasks available on this page.

Network > Routes Overview

The **Network > Routes** page allows the administrator to assign a default gateway and interface, and to add and configure static routes. For more information on default or static routes, refer to the *SonicWALL SSL VPN Getting Started Guide* for your appliance model.

Figure 18 SSL-VPN models 2000 or higher Network > Routes Page

Default Route

The default route section allows the administrator to define the default network route by setting the default IPv4 gateway and interface, and/or default IPv6 (for SSL-VPN models 2000 and higher) gateway and interface. The number of interfaces differs among appliance models (X0, X1, X2, X3 for SSL-VPN 2000; X0, X1, X2, X3, X4, X5 for SSL-VPN 4000). A default network route is required for Internet access.

Static Routes

The static routes section allows the administrator to add and configure additional static routes by specifying a destination network, subnet mask, optional default gateway, and interface. IPv6 static routes are supported on SonicWALL SSL-VPN models 2000 and higher.

Destination IPv6 Network	Prefix	Gateway	Interface	Delete
2007:1:2::	64	2007::1:2:3:1	X1	⊗

Configuring a Default Route for the SSL-VPN Appliance

You must configure a default gateway on your SonicWALL SSL-VPN appliance for it to be able to communicate with remote networks. A remote network is any IP subnet different from its own. In most cases, the default gateway will be the LAN IP address of the SonicWALL firewall interface to which the SonicWALL SSL-VPN is connected. IPv6 is supported for the default gateway on SonicWALL SSL-VPN models 2000 and higher. This is the default route for the appliance.

To configure the default route, perform the following steps:

Step 1 Navigate to the **Network > Routes** page.

Step 2 In the **Default IPv4 Gateway** field, type the IP address of the firewall or other gateway device through which the SonicWALL SSL-VPN connects to the network. This address will act as the default route for the appliance.

Step 3 In the **Interface** drop-down list, select the interface that will serve as the IPv4 connecting interface to the network. In most cases, the interface will be X0.

Step 4 On a SonicWALL SSL-VPN model 2000 or higher, in the **Default IPv6 Gateway** field, type the IPv6 address of the firewall or other gateway device through which the SonicWALL SSL-VPN connects to the network. This address will act as the default IPv6 route for the appliance.

Step 5 In the **Interface** drop-down list, select the interface that will serve as the IPv6 connecting interface to the network.

Step 6 Click **Accept**.

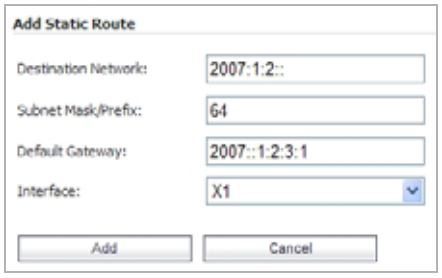
Configuring Static Routes for the Appliance

Based on your network's topology, you might find it necessary or preferable to configure static routes to certain subnets rather than attempting to reach them through the default gateway. While the default route is the default gateway for the device, static routes can be added as needed to make other networks reachable for the SonicWALL SSL-VPN appliance. For more details on routing or static routes, refer to a standard Linux reference guide.

To configure a static route to an explicit destination for the appliance, perform the following steps:

Step 1 Navigate to the **Network > Routes** page and click the **Add Static Route...** button.

Step 2 In the **Add Static Route** dialog box on the SonicWALL SSL-VPN model 2000 or higher, type the subnet or host to which the static route will be directed into the **Destination Network** field (for example, **192.168.220.0** provides a route to the 192.168.220.X/24 subnet). You can enter an IPv6 subnet (for example, **2007:1:2::**).



Step 3 In the **Subnet Mask/Prefix** field, enter the number of bits used for the prefix.

Step 4 In the **Default Gateway** field, type the IP address of the gateway device that connects the appliance to the network. On a SonicWALL SSL-VPN model 2000 or higher, you can enter an IPv6 address.

Step 5 In the **Interface** drop-down list, select the interface that connects the appliance to the desired destination network.

Step 6 Click **Add**.

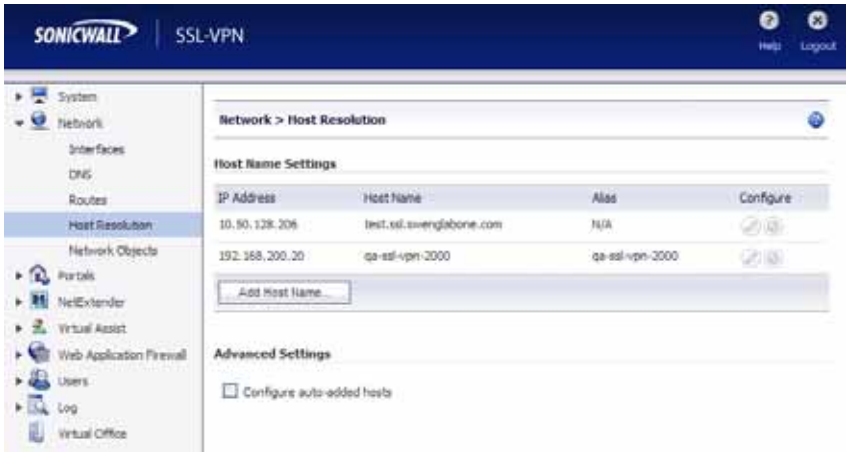
Network > Host Resolution

This section provides an overview of the **Network > Host Resolution** page and a description of the configuration tasks available on this page.

Network > Host Resolution Overview

The **Network > Host Resolution** page allows the administrator to configure host names.

Figure 19 SSL-VPN models 2000 or higher Network > Host Resolution Page



Host Name Settings

The host name settings section allows the administrator to add and configure a host name by specifying an IP address, host name (host or FQDN) and an optional alias.

Configuring Host Resolution

The Host Resolution page enables network administrators to configure or map host names or fully qualified domain names (FQDNs) to IP addresses.

Note A host resolution entry is automatically created for the SonicWALL SSL-VPN appliance itself. Do not delete it.

The SonicWALL SSL-VPN appliance can act as both a NetBIOS and WINS (Windows Internet Name Service) client to learn local network host names and corresponding IP addresses.

To resolve a host name to an IP address, perform the following steps:

Step 1 Navigate to the **Network > Host Resolution** page. The **Network** > **Host Resolution** page is displayed.

Step 2 Click **Add Host Name**. The **Add Host Name** dialog box is displayed.

Step 3 In the **Add Host Name** dialog box, in the **IP Address** field, type the IP address that maps to the hostname.

Step 4 In the **Host Name** field, type the hostname that you want to map to the specified IP address.

Step 5 Optionally, in the **Alias** field, type a string that is the alias for the hostname.

Step 6 Click **Add**. The **Host Resolution** page now displays the new host name.

Step 7 On a SonicWALL SSL-VPN model 2000 or higher, optionally select the **Configure auto-added hosts** checkbox on the **Network > Host Resolution** page. If this option is selected, you can edit or delete automatically added Host entries (such as for IPv6). This option is not recommended, as host mis-configuration could lead to undesirable results.

Network > Network Objects

This section provides an overview of the **Network > Network Objects** page and a description of the configuration tasks available on this page.

- "Network > Network Objects Overview" section on page 100
- "Configuring Network Objects" section on page 101

Network > Network Objects Overview

The **Network > Network Objects** page allows the administrator to add and configure network resources, called objects. For convenience, you can create an entity that contains both a service and an IP address mapped to it. This entity is called a network object. This creates an easy way to specify a service to an explicit destination (the network object) when you are applying a policy, instead of having to specify both the service and the IP address.

On SonicWALL SSL-VPN model 2000 or higher appliances, you can create IPv6 network objects using IPv6 object types and addresses.

Figure 20 SSL-VPN models 2000 or higher Network > Network Objects Page

Network objects are set up by specifying a name and selecting one of the following services:

- Web (HTTP)
- Secure Web (HTTPS)
- NetExtender
- Terminal Services (RDP - Active X)

- Terminal Services (RDP - Java)
- Virtual Network Computing (VNC)
- File Transfer Protocol (FTP)
- Telnet, Secure Shell version 1 (SSHv1) / Secure Shell version 2 (SSHv2)
- File Shares (CIFS)
- Citrix Portal (Web Access)

Port or port range settings are available for all services, allowing the administrator to configure a port range (such as 80-443) or a port number (80) for a Network Object. You can use this feature to create port-based policies. For example, you can create a Deny All policy and allow only HTTP traffic to reach port 80 of a Web server.

Configuring Network Objects

To create a network object, perform the following steps:

Step 1 Navigate to the **Network** > **Network Objects** page.

Step 2 Click the **Add Network Object...** button. The **Add Network Object** dialog box is displayed.

Step 3 Type a string in the **Name** field that will be the name of the network object you are creating.

Note To edit an existing network object, select the configure button next to the object you want to edit. A new network object with the same name as an existing network object will not replace or modify the existing network object.

Step 4 Click on the **Service** list and select a service type: Web (HTTP), Secure Web (HTTPS), NetExtender, Terminal Services (RDP - Java), Terminal Services (RDP - ActiveX), Virtual Network Computing, File Transfer Protocol, Telnet, Secure Shell version 1 (SSHv1), Secure Shell version 2 (SSHv2, which provides stronger encryption than SSHv1 and can only connect to a server that support SSHv2), File Shares (CIFS), or Citrix.

Step 5 Click **Add**. The **Network** > **Network Objects** page is displayed with the new network object in the **Network Objects** list.

Step 6 If the object is not fully defined with at least one IP address or network range, the status **Incomplete** will display.

Note Policies cannot be created for incomplete network objects.

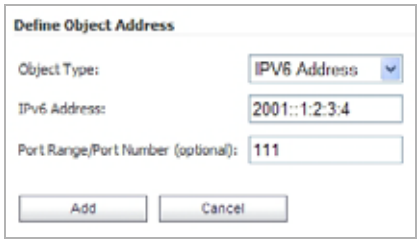
Step 7 To assign an address to the network object you just created, or to edit an existing network object, click on the **Configure** icon or click the **Incomplete** link. The **Edit Network Object** dialog box is displayed, showing the network object name and the service associated with it. It also contains an address list that displays existing addresses mapped to the network object.

Step 8 To change the service, select the desired service from the **Service** drop-down list and then click **Update Service**. The Service column in the Network Objects table displays the new service, and the **Edit Network Object** dialog box remains open. You can click **Close** if finished.

Step 9 To add Type and Address values for this Network Object, click **Add**. The **Define Object Address** dialog box is displayed.

Step 10 In the **Define Object Address** dialog box on the SonicWALL SSL-VPN model 2000 or higher, click on the **Object Type** drop-down list and select an object type. The four object types are:

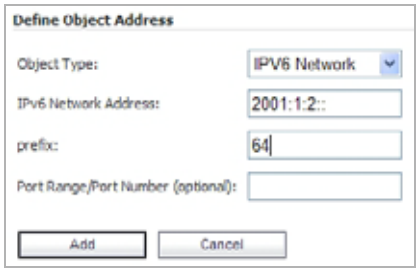
- **IP Address** - A single IP address.
- **Network Address** - A range of IP addresses, defined by a starting address and a subnet mask.
- **IPV6 Address** - A single IPv6 address.
- **IPV6 Network** - A range of IPv6 addresses.



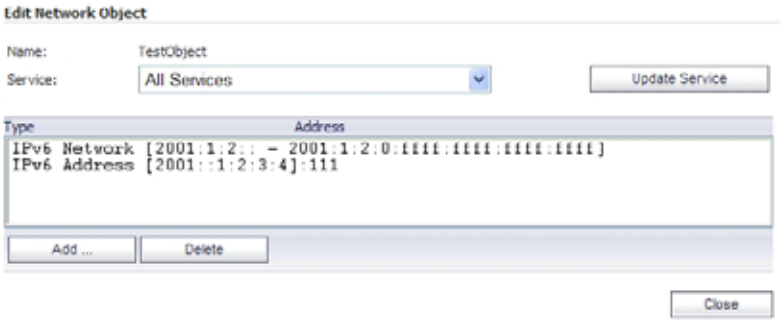
Step 11 Type in the appropriate information pertaining to the object type you have selected.

- For the **IP Address** object type, type an IP address in the **IP Address** field.
- For the **IP Network** object type, in the **Network Address** field, type an IP Address that resides in the desired network subnet and type a subnet mask in the **Subnet Mask** field.In the **Port Range/Port Number** field, optionally enter a port range in the format 80-443, or enter a single port number.
- For the **IPV6 Address** object type, type an IP address in the **IPv6 Address** field.

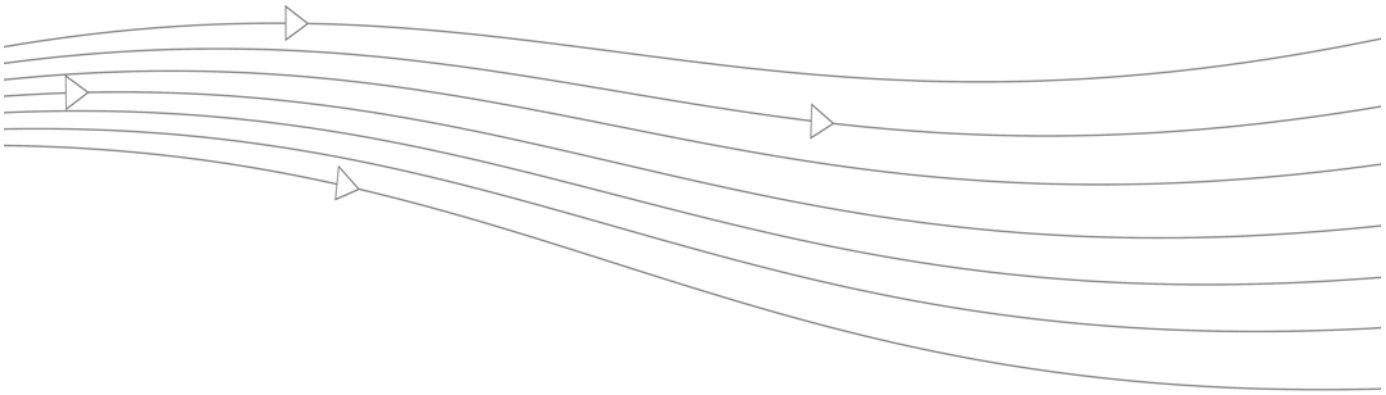
– For the **IPV6 Network** object type, in the **IPv6 Network Address** field, type an IPv6 address that resides in the desired network subnet and type the number of bits to use as a prefix in the **Prefix** field.



Step 12 Click **Add**.



Step 13 When finished adding addresses, click **Close** in the Edit Network Object dialog box.



Chapter 4: Portals Configuration

This chapter provides information and configuration tasks specific to the **Portals** pages on the SonicWALL SSL VPN Web-based management interface, including configuring portals, assigning portals, and defining authentication domains, such as RADIUS, NT Domain, LDAP, and Active Directory.

This chapter contains the following sections:

Portals > Portals

This section provides an overview of the **Portals > Portals** page and a description of the configuration tasks available on this page.

For information about Application Offloading and the **Offload Web Application** button, see the "Portals > Application Offloading" section on page 118.

Portals > Portals Overview

The **Portals > Portals** page allows the administrator to configure a custom portal for the SSL VPN Portal login page as well as the portal home page.

Figure 21 Portals > Portals on SSL-VPN models 2000 or higher

Portal Settings

The **Portal Settings** section allows the administrator to configure a custom portal by providing the portal name, portal site title, portal banner title, login message, virtual host/domain name and portal URL. This section also allows the administrator to configure custom login options for control over what is displayed/loaded on login and logout, HTTP meta tags for cache control, ActiveX Web cache cleaner and login uniqueness.

Legacy portals are indicated in the Description column. These portals retain the classic interface from SonicOS SSL VPN releases prior to 3.5. The administrator may choose to keep a legacy portal rather than upgrade it if the portal has been customized or for other reasons.

Additional Information About the Portal Home Page

For most SonicWALL SSL VPN administrators, a plain text home page message and a list of links to network resources is sufficient. For administrators who want to display additional content on the user portal, review the following information.

Modern Portals

- With the Tips/Help sidebar enabled, the width of the workspace is 561 pixels.
- With the Tips/Help sidebar disabled, the width of the workspace is 712 pixels.
- No IFRAME is used.
- You can upload a custom HTML file which will be displayed below all other content on the home page. You can also add HTML tags and JavaScript to the **Home Page Message** field.
- Since the uploaded HTML file will be displayed after other content, do not include <head> or <body> tags in the file.

Legacy Portals

- The home page is displayed in an IFRAME--internal HTML frame.
- The width of the iframe is 542 pixels, but since there is a 29 pixel buffer between the navigation menu and the content, the available workspace is 513 pixels.
- You can upload a custom HTML file which will be displayed below all other content on the home page. You can also add HTML tags and JavaScript to the **Home Page Message** field.
- Since the uploaded HTML file will be displayed after other content, do not include <head> or <body> tags in the file.

Adding Portals

The administrator can customize a portal that appears as a customized landing page to users when they are redirected to the SonicWALL SSL VPN for authentication.

The network administrator may define individual layouts for the portal. The layout configuration includes menu layout, portal pages to display, portal application icons to display, and Web cache control options.

The default portal is the **Virtual Office** portal. Additional portals can be added and modified. To add a portal, perform the following steps:

Step 1 Navigate to the **Portals > Portals** window and click the **Add Portal** button. The **Portal Settings** window is displayed.

Table 9 provides a description of the fields you may configure on the **General** tab. Refer to "Configuring General Portal Settings" section on page 109 for the specific steps required to configure a custom portal.

Table 9 General Tab Fields.

Field	Description
Portal Name	The title used to refer to this portal. It is for internal reference only, and is not displayed to users.
Portal Site Title	The title that will appear on the Web browser title bar of users access this portal.
Portal Banner Title	The welcome text that will appear on top of the portal screen.
Login Message	Optional text that appears on the portal login page above the authentication area.
Virtual Host/Domain Name	Used in environments where multiple portals are offered, allowing simple redirection to the portal URL using virtual hosts. This option is only available on SonicWALL SSL-VPN models 2000 and higher.
Portal URL	The URL that is used to access this specific portal.
Display custom login page	Displays the customized login page rather than the default (SonicWALL) login page for this portal.
Display login message on custom login page	Displays the text specified in the Login Message text box.
Enable HTTP meta tags for cache control	Enables HTTP meta tags in all HTTP/HTTPS pages served to remote users to prevent their browser from caching content.

Field	Description
Enable ActiveX Web cache cleaner	Loads an ActiveX control (browser support required) that cleans up all session content after the SonicWALL SSL VPN session is closed.
Enforce login uniqueness	If enforced, login uniqueness restricts each account to one session at a time. If not enforced, each account can have multiple simultaneous sessions.

Configuring General Portal Settings

There are two main options for configuring a portal:

- Modify an existing layout.
- Configure a new portal.

To configure the settings on the General tab for a new portal, perform the following steps:

Step 1 Navigate to the **Portals > Portals** page.

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 On the General tab, enter a descriptive name for the portal in the **Portal Name** field. This name will be part of the path of the SonicWALL SSL-VPN appliance portal URL. For example, if your SonicWALL SSL-VPN portal is hosted at **https://vpn.company.com**, and you created a portal named “sales”, then users will be able to access the sub-site at **https://vpn.company.com/portal/sales**.

Note Only alphanumeric characters, hyphen (-), and underscore (_) are accepted in the **Portal Name** field. If other types of characters or spaces are entered, the portal name will be truncated before the first non-alphanumeric character.

Step 4 Enter the title for the Web browser window in the **Portal Site Title** field.

Step 5 To display a banner message to users before they login to the portal, enter the banner title text in the **Portal Banner Title** field.

Step 6 Enter an HTML compliant message, or edit the default message in the **Login Message** field. This message is shown to users on the custom login page.

Step 7 The **Portal URL** field is automatically populated based on your SSL-VPN network address and Portal Name.

Step 8 To enable visibility of your custom logo, message, and title information on the login page, select the **Display custom login page** checkbox.

Note Custom logos can only be added to existing portals. To add a custom logo to a new portal, first complete general portal configuration, then add a logo. On a SSL-VPN model 2000 or higher, follow the procedures in the “Adding a Custom Portal Logo” section on page 116.

Step 9 Select the **Enable HTTP meta tags for cache control** checkbox to apply HTTP meta tag cache control directives to the portal. Cache control directives include:

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

These directives help prevent clients browsers from caching SonicWALL SSL VPN portal pages and other Web content.

Note Enabling HTTP meta tags is strongly recommended for security reasons and to prevent out-of-date Web pages, and data being stored in users' Web browser cache.

Step 10 Select the **Enable ActiveX Web cache cleaner** checkbox to load an ActiveX cache control when users log in to the SonicWALL SSL-VPN appliance. The Web cache cleaner will prompt the user to delete all session temporary Internet files, cookies and browser history when the user logs out or closes the Web browser window. The ActiveX Web cache control is ignored by Web browsers that don't support ActiveX.

Step 11 See "Enforcing Login Uniqueness" on page 110.

Step 12 See "Configuring the Home Page" on page 110.

Enforcing Login Uniqueness

Login uniqueness, when enforced, restricts each account to a single session at a time. When login uniqueness is not enforced, each account can have multiple, simultaneous, sessions. To enforce login uniqueness, perform the following steps:

Step 1 Navigate to **Portals > Portals.**

Step 2 For an existing portal, click the configure icon next to the portal you want to configure. Or, for a new portal, click the **Add Portal** button.

Step 3 Select the **Enforce login uniqueness** checkbox.

Step 4 Click **OK**.

Configuring the Home Page

The home page is an optional starting page for the SonicWALL SSL-VPN appliance portal. The home page enables you to create a custom page that mobile users will see when they log into the portal. Because the home page can be customized, it provides the ideal way to communicate remote access instructions, support information, technical contact information or SSL VPN-related updates to remote users.

The home page is well-suited as a starting page for restricted users. If mobile users or business partners are only permitted to access a few files or Web URLs, the home page can be customized to show only those links.

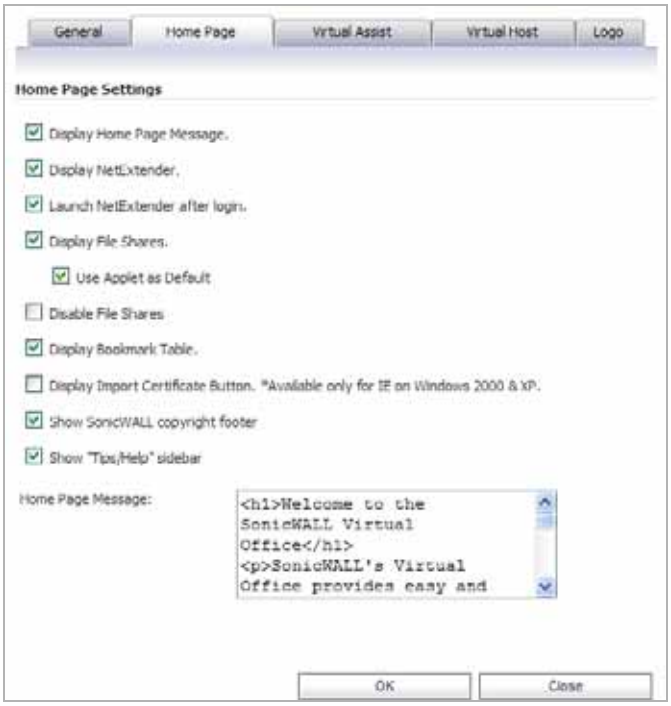
You can edit the title of the page, create a home page message that is displayed at the top of the page, show all applicable bookmarks (user, group, and global) for each user, and optionally upload an HTML file.

To configure the home page, perform the following tasks:

Step 1 Navigate to the **Portals > Portals** page.

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 Click the **Home Page** tab.



Step 4 Table 10 provides a description of the configurable options in the **Home Page** tab.

Table 10 Home Page Tab Fields

Field	Description
Display Home Page Message	Displays the customized home page message after a user successfully authenticates to the SonicWALL SSL-VPN appliance.
Display NetExtender	Displays the link to NetExtender, allowing users to install and invoke the clientless NetExtender virtual adapter.
Launch NetExtender after Login	Launches NetExtender automatically after a user successfully authenticates to the SonicWALL SSL-VPN appliance. See “Enabling NetExtender to Launch Automatically in the User Portal” section on page 113.
Display File Shares	Provide a link to the File Shares (Windows CIFS/SMB) Web interface so that authenticated SonicWALL SSL VPN users may use NT file shares according to their domain permissions. See “File Sharing Using “Applet as Default”” section on page 113
Use Applet as Default	Enables the Java File Shares Applet, giving users a simple yet powerful file browsing interface with drag-and-drop, multiple file selection and contextual click capabilities.

Field	Description
Disable File Shares	Prevents access to all File Shares including the File Shares Applet and the File Shares HTML interface. The File Shares link will not be displayed on the portal. Selecting this option automatically disables the Display Files Shares and Use Applet as Default checkboxes.
Display Bookmark Table	Displays the bookmark table containing administrator-provided bookmarks and allows users to define their own bookmarks to network resources.
Display Import Certificate Button	Displays a button that allows users to permanently import the SSL security certificate. Certificate import is only available for Internet Explorer on Windows 2000 and XP.
Show SonicWALL copyright footer	Displays SonicWALL copyright footer on portal. If unchecked, the footer is not shown.
Show “Tips/Help” sidebar	Displays a sidebar in the portal with tips and help links. This option is not available when the Legacy Look & Feel checkbox is selected on the General tab.
Home Page Message	Optional text that can be displayed on the home page after successful user authentication.
Bookmark Table Title	Optional text to describe the bookmark section on the portal’s home page. This field is only displayed when the Legacy Look & Feel checkbox is selected on the General tab.

Note When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SonicWALL SSL-VPN is not a domain member and will not be able to connect to the DFS shares.
DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

Note Some ActiveX applications, such as the ActiveX Terminal Services RDP client, will only work when connecting to a server with a certificate from a trusted root authority. If you are using the test SSL certificate that is included with the SonicWALL SSL-VPN appliance, then you can select the **Display Import self-signed certificate links** checkbox to allow Windows users to easily import a self-signed certificate.

It is strongly recommended that you upload a valid SSL certificate from a trusted root authority such as Verisign or Thawte. If you have a valid SSL certificate, do not select the **Display Import self-signed certificate links** checkbox.

Step 5 Click **OK** to update the home page content.

Enabling NetExtender to Launch Automatically in the User Portal

NetExtender can be configured to start automatically when a user logs into the user portal. You can also configure whether or not NetExtender is displayed on a Virtual Office portal. To configure NetExtender portal options, perform the following steps:

Step 1 Navigate to **Portals > Portals**

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 Click the **Home Page** tab.

Step 4 To prevent users from accessing NetExtender through this portal, clear the **Display NetExtender** checkbox.

Step 5 To launch NetExtender automatically when users login to the portal, select the **Launch NetExtender after login** checkbox.

Step 6 Click **OK**.

File Sharing Using “Applet as Default”

The Java File Shares Applet option provides users with additional functionality not available in standard HTML-based file sharing, including:

- Overwriting of existing files
- Uploading directories
- Drag-and-drop capability
- Multiple file selection
- Contextual click capability
- Sortable file listings
- Ability to navigate directly to folders by entering path
- Back and forward buttons with a drop-down history menu
- Properties window displays folder size

To use the Java File Shares Applet on this portal, perform the following tasks:

Step 1 Navigate to **Portals > Portals**.

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 Click the **Home Page** tab.

Step 4 Select the **Display File Shares** checkbox.

Step 5 Select the **Use Applet as Default** checkbox.

Step 6 Click the **OK** button to save changes.

Configuring Per-Portal Virtual Assist Settings

(Virtual Assist is supported only on SonicWALL SSL-VPN models 2000 and higher.) The administrator can enable Virtual Assist on a per-portal basis. This option is only available on SonicWALL SSL-VPN models 2000 and higher.

The Virtual Assist tab in the Add Portal screen provides almost the same configuration options for this portal as are offered by the global Virtual Assist > Settings page.

To configure the Virtual Assist settings for this portal, perform the following steps:

Step 1 Navigate to **Portals > Portals**.

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 Click the **Virtual Assist** tab.

Step 4 To allow Virtual Assist on this portal, select the **Enable Virtual Assist for this Portal** checkbox.

Step 5 Select the **Display Technician Button** checkbox. If this box is not selected, the Virtual Assist button will be hidden and technicians will be required to login directly through a downloaded client.

Step 6 Select the **Display Request Help Button** checkbox to allow users to request assistance through the portal.

Step 7 Select the **Enable Virtual Access Mode** checkbox to allow Virtual Access connections to be made to this portal. This must be enabled per-portal for Virtual Access to function. If this box is selected, you can then select the **Display Virtual Access Setup Link** checkbox to display the corresponding link on the portal. For more information on Virtual Access functionality, see "Enabling a System for Virtual Access" on page 41.

Step 8 In the **Limit Support Sessions** field, enter the number of active support sessions allowed on this portal, or enter zero for no limitation.

Step 9 See "Virtual Assist > Settings" on page 171 for information about all other configuration settings on the Virtual Assist tab.

Step 10 For the fields with a drop-down list, do one of the following:

- Select **Use global setting** to apply the global setting to this portal.
- Select **Enable** to enable the option for this portal, no matter what the global setting is.
- Select **Disable** to disable the option for this portal, no matter what the global setting is.

Step 11 For fields without a drop-down list, you can leave the field blank to use the global settings for this portal.

Step 12 Click the **OK** button to save changes.

Configuring Virtual Host Settings

(Virtual Host is supported only on SonicWALL SSL-VPN models 2000 and higher.) Creating a virtual host allows users to log in using a different hostname than your default URL. For example, sales members can access **https://sales.company.com** instead of the default domain, **https://vpn.company.com** that you use for administration. The Portal URL (for example, **https://vpn.company.com/portal/sales**) will still exist even if you define a virtual host name. Virtual host names enable administrators to give separate and distinct login URLs to different groups of users. This option is only available on SonicWALL SSL-VPN models 2000 and higher.

To create a Virtual Host Domain Name, perform the following tasks:

Step 1 Navigate to **Portals > Portals**.

Step 2 Click the **Add Portal** button or the configure button next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.

Step 3 Click the **Virtual Host** tab.

Step 4 Enter a host name in the **Virtual Host Domain Name** field, for example, **sales.company.com**. This field is optional.

Note Only alphanumeric characters, hyphen (-) and underscore (_) are accepted in the **Virtual Host Name/Domain Name** field.

Step 5 Select a specific **Virtual Host Interface** for this portal if using IP based virtual hosting.

Note If your virtual host implementation uses name based virtual hosts — where more than one hostname resides behind a single IP address — choose **All Interfaces** from the Virtual Host interface.

Step 6 If you selected a specific Virtual Host Interface for this portal, enter the desired **Virtual Host IP Address** in the field provided. This is the IP address users will access in order to access the Virtual Office portal.

Note Be sure to add an entry in your external DNS server to resolve the virtual hostname and domain name to the external IP address of your SonicWALL SSL-VPN appliance.

Step 7 If you selected a specific Virtual Host Interface for this portal, you can specify an IPv6 address in the **Virtual Host IPv6 Address** field (on SonicWALL SSL-VPN models 2000 and higher only). You can use this address to access the virtual host. Enter the IPv6 address using decimal or hexadecimal numbers in the form:

2001::A987:2:3:4321

Step 8 If you plan to use a unique security certificate for this sub-domain, select the corresponding port interface address from the **Virtual Host Certificate** list.

Note Unless you have a certificate for each virtual host domain name, or if you have purchased a *.domain SSL certificate, your users may see a **Certificate host name mismatch** warning when they log into the SonicWALL SSL-VPN appliance portal. The certificate hostname mismatch only affects the login page; SonicWALL SSL VPN client applications will not be affected by a hostname mismatch.

Adding a Custom Portal Logo

On SonicWALL SSL-VPN models 2000 and higher, the Custom Logo Settings section allows the administrator to upload a custom portal logo and to toggle between the default SonicWALL logo and a custom uploaded logo. You must add the portal before you can upload a custom logo. In the Add Portal screen, the Logo tab does not have an option to upload a custom logo.

To add a custom portal logo, perform the following steps:

Step 1 Navigate to **Portals > Portals** and click the configure button next to the existing portal to which you want to add a custom logo. The **Edit Portal** screen displays.

Step 2 Click the **Logo** tab.

Step 3 Click the **Browse...** button next to the **Upload Logo** field. The file browser window displays.

Step 4 Select a proper sized .gif format logo in the file browser and click the **Open** button.

Note The custom logo must be in GIF format. In a modern portal, there is a hard size limit of 155x68 pixels. Anything larger than this will be cropped to fit the designated logo space on the page. In a legacy portal, for the best aesthetic results, import a logo with a transparent or light-colored background. The recommended, but not mandatory, size is 155x36 pixels.

Step 5 Select **Light** or **Dark** from the **Background** drop-down list. Select a background shade that will help set off your logo from the rest of the portal page.

Step 6 Click the **Update Logo** button to transfer the logo to the SSL-VPN appliance.

Step 7 Click the **Default Logo** button to revert to the default SonicWALL logo.

Step 8 Click the **OK** button to save changes.

Portals > Application Offloading

(Application Offloading is supported only on SonicWALL SSL-VPN models 2000 and higher.) The Portals > Application Offloading page in the management interface provides an overview of the Application Offloading functionality available from the Portals > Portals page. No configuration is available on this page.

Click any of the screenshots on this page to go to the Portals > Portals page, where you can click the **Offload Web Application** button to configure an offloaded application.

See the following sections:

- "Application Offloading Overview" on page 118
- "Configuring an Offloaded Application" on page 119

Application Offloading Overview

Application Offloading provides secure access to both internal and publicly hosted Web applications. An application offloading host is created as a special-purpose portal with an associated virtual host acting as a proxy for the backend Web application.

Unlike HTTP(S) bookmarks, access to offloaded applications is not limited to remote users. The administrator can enforce strong authentication and access policies for specific users or groups. For instance, in an organization certain guest users may need Two-factor or Client Certificate authentication to access Outlook Web Access (OWA), but are not allowed to access OWA public folders. If authentication is enabled, multiple layers of SonicWALL advanced authentication features such as One Time Password, Two-factor Authentication, Client Certificate Authentication and Single Sign-On can be applied on top of each other for the offloaded host.

The portal must be configured as a virtual host with a suitable SSL VPN domain. It is possible to disable authentication and access policy enforcement for such an offloaded host.

Web transactions can be centrally monitored by viewing the logs. In addition, Web Application Firewall can protect these hosts from any unexpected intrusion, such as Cross-site scripting or SQL Injection.

Access to offloaded Web applications happens seamlessly as URLs in the proxied page are not rewritten in the manner used by HTTP or HTTPS bookmarks.

An offloaded Web application has the following advantages over configuring the Web application as an HTTP(S) bookmark in SSL VPN:

- No URL rewriting is necessary, thereby improving the throughput tremendously.
- The functionality of the original Web application is retained almost completely, while an HTTP(S) bookmark is only a best-effort solution.
- Application offloading extends SSL VPN security features to publicly hosted Web sites.

Application offloading can be used in any of the following scenarios:

- To function as an SSL offloader and add HTTPS support to the offloaded Web application, using the integrated SSL accelerator hardware of the SSL-VPN appliance.
- In conjunction with the Web Application Firewall subscription service to provide the offloaded Web application continuous protection from malicious Web attacks.
- To add strong or stacked authentication to the offloaded Web application, including Two-factor authentication, One Time Passwords and Client Certificate authentication.

- To control granular access to the offloaded Web application using global, group or user based access policies.
- To support Web applications not currently supported by HTTP/HTTPS bookmarks. Application Offloading does not require URL rewriting, thereby delivering complete application functionality without compromising throughput.

Note The Application Offloading feature will not work well if the application refers to resources within the same host using absolute URLs. In this case, you may need to convert an absolute URL reference to its relative form.

Note NTLM (Microsoft NT Lan Manager) authentication and digest authentication schemes are not supported for HTTP(S) bookmarks or Application Offloading.

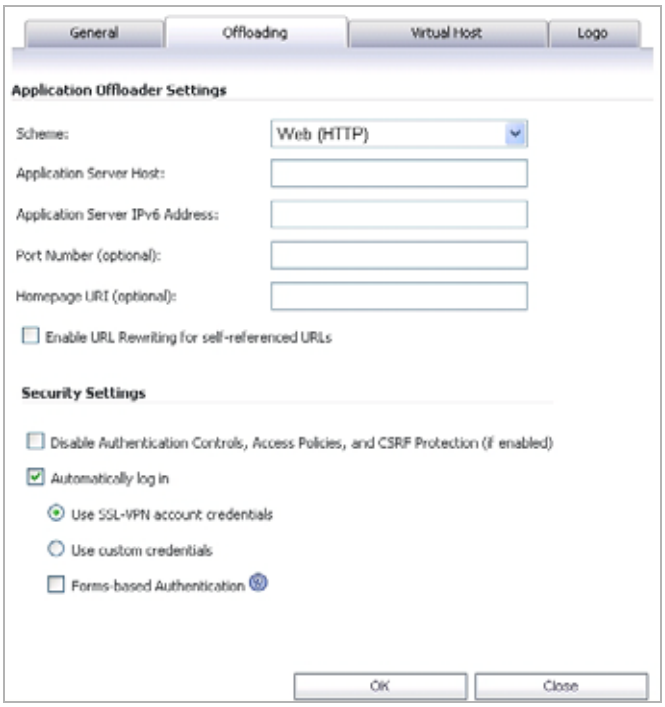
Further information about configuring specific backend Web applications is available in the Reverse Proxy feature module, available at:

http://www.sonicwall.com/downloads/SSL_VPN_3.5_Reverse_Proxy.pdf

Configuring an Offloaded Application

On SonicWALL SSL-VPN models 2000 and higher, to offload a Web application, perform the following steps:

Step 1 Navigate to **Portals > Portals** and click the **Offload Web Application** button. The Add Portal screen opens. The screen contains the **Offloading** tab, used specifically for application offloading configuration.



Step 2 On the **General** tab, enter a descriptive name in the **Portal Name** field. See the "Configuring General Portal Settings" section on page 109 for more instructions for configuring the fields on this tab.

Step 3 On the **Offloading** tab, select one of the following from the Scheme drop-down list:

- **Web (HTTP)** – access the Web application using HTTP
- **Secure Web (HTTPS)** – access the Web application using HTTPS

Step 4 Enter the host name or private IP address of the backend host into the **Application Server Host** field.

Step 5 Optionally enter the IPv6 address of the backend host into the **Application Server IPv6 Address** field.

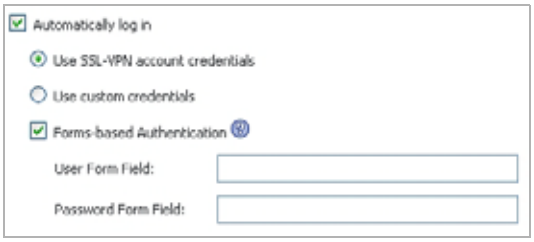
Step 6 In the **Port Number (optional)** field, optionally enter a custom port number to use for accessing the application.

Step 7 In the **Homepage URI (optional)** field, optionally enter a URI to a specific resource on the Web server to which the user will be forwarded after logging in. This is a string in the form of: **/exch/test.cgi?key1=value1&key2=value2**

Step 8 Select the **Enable URL Rewriting for self-referenced URLs** checkbox if you want absolute URLs that refer to this application server in HTML, Javascript, or CSS content to be rewritten.

Step 9 Under Security Settings, select the **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** checkbox if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.

Step 10 Select the **Automatically Login** checkbox to configure Single Sign-On settings.



Step 11 For automatic login, select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow login to the offloaded application using the credentials configured on the SSL-VPN appliance
- **Use custom credentials** – displays **Username**, **Password**, and **Domain** fields where you can enter the custom credentials for the application or use dynamic variables such as those shown below:

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%

Step 12 If you selected **Automatically Login**, select the **Forms-based Authentication** checkbox to configure Single Sign-On for forms-based authentication.

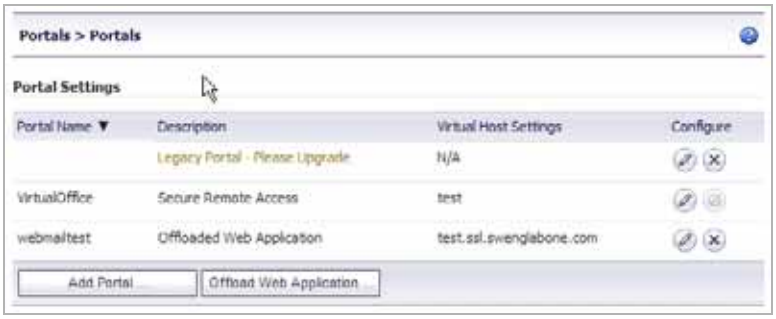
- Configure the **User Form Field** to be the same as the 'name' and 'id' attribute of the HTML element representing User Name in the Login form, for example:
  <input type=text name='userid'>
- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:
  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>

Step 13 On the **Virtual Host** tab, set a host name for the application in the **Virtual Host Domain Name** field, and optionally enter a descriptive alias in the **Virtual Host Alias** field.

If you need to associate a certificate to this host, you should additionally set a virtual interface and import the relevant SSL certificate. You could avoid creating a virtual interface by importing a wildcard certificate for all virtual hosts on the SSL-VPN.

See the "Configuring Virtual Host Settings" section on page 115 for more instructions on configuring the fields on this tab.

Step 14 Click **OK**. You are returned to the Portals > Portals page where you will see the Web application listed as an **Offloaded Web Application** under Description.



Step 15 If you have not disabled authentication, navigate to the **Portals > Domains** page and create a domain for this portal. See the "Portals > Domains" section on page 122 for information about creating a domain.

Step 16 Update your DNS server for this virtual host domain name and alias (if any).

Portals > Domains

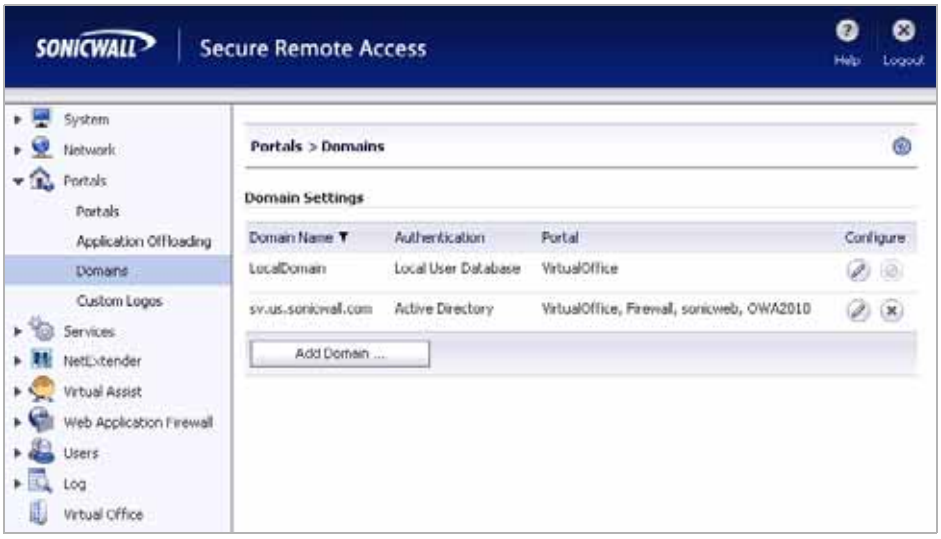
This section provides an overview of the **Portals > Domains** page and a description of the configuration tasks available on this page.

Portals > Domains Overview

The **Portals > Domains** page allows the administrator to add and configure a domain. The **Portals > Domains** page allows the administrator to add and configure a domain by selecting:

- Authentication type (local user database, Active Directory, LDAP, NT Domain, or RADIUS),
- Domain name
- Portal name
- Group (AD, RADIUS) or multiple Organizational Unit (LDAP) support (optional)
- Require client digital certificates (optional)
- One-time passwords (optional)

Figure 22 Portals > Domains Page



Domain Settings

The domain settings section allows the administrator to add a domain by selecting an authentication type (local user database, Active Directory, LDAP, NT Domain, or RADIUS), specifying a domain name, selecting a portal name, and optionally selecting require client digital certificates and one-time passwords.

Adding a Domain with Local User Database Authentication

Note After adding a new portal domain, user group settings for that domain are configured on the **Users > Local Groups** page. Refer to the "Users > Local Groups" section on page 227 for instructions on configuring groups.

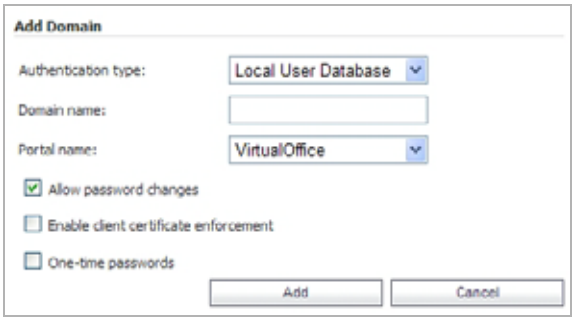
In order to create access policies, you must first create authentication domains. By default, the LocalDomain authentication domain is already defined. The LocalDomain domain is the internal user database. Additional domains may be created that require authentication to remote authentication servers. SonicWALL SSL VPN supports RADIUS, LDAP, NT Domain, and Active Directory authentication in addition to internal user database authentication.

Note To apply a portal to a domain, add a new domain and select the portal from the Portal Name drop-down list in the **Add Domain** dialog box. The selected portal will be applied to all users in the new domain.Domain choices will only be displayed in the login page of the Portal that was selected.

You may create multiple domains that authenticate users with user names and passwords stored on the SonicWALL SSL-VPN appliance to display different portals (such as a SonicWALL SSL VPN portal page) to different users.

To add a domain for local database authentication, perform the following steps:

Step 1 Navigate to the **Portals > Domains** window and click the **Add Domain** button. The **Add Domain** window is displayed.



Step 2 Select **Local User Database** from the **Authentication Type** drop-down list.

Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL VPN portal.

Step 4 Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

Step 5 Optionally, select the **Allow password changes** checkbox. This allows users to change their own passwords after their account is set up.

Step 6 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 7 Optionally select the **One-time passwords** checkbox to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

Step 8 If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

Step 9 Click **Add** to update the configuration. Once the domain has been added, the domain will be added to the **Domain Settings** table.

Adding a Domain with RADIUS Authentication

To create a domain with RADIUS authentication, perform the following steps:

Step 1 On the **Portals > Domains** page, click **Add Domain** to display the **Add Domain** dialog box.

Step 2 Select **RADIUS** from the **Authentication Type** menu. The **RADIUS configuration** field is displayed.

Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL-VPN appliance portal.

Step 4 Select the proper **Authentication Protocol** for your RADIUS server. Choose from **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPV2**.

Step 5 Under **Primary Radius Server**, enter the IP address or domain name of the RADIUS server in the **RADIUS Server Address** field.

Step 6 Enter the RADIUS server port in the **RADIUS server port** field.

Step 7 If required by your RADIUS configuration, enter an authentication secret in the **Secret Password** field.

Step 8 Enter a number (in seconds) for RADIUS timeout in the **RADIUS Timeout (Seconds)** field.

Step 9 Enter the maximum number of retries in the **Max Retries** field.

Step 10 Under **Backup Radius Server**, enter the IP address or domain name of the backup RADIUS server in the **RADIUS Server Address** field.

Step 11 Enter the backup RADIUS server port in the **RADIUS server port** field.

Step 12 If required by the backup RADIUS server, enter an authentication secret for the backup RADIUS server in the **Secret Password** field.

Step 13 Optionally, if using RADIUS for group-based access, select the **Use Filter-ID for RADIUS Groups** checkbox.

Step 14 Click the name of the layout in the **Portal Name** drop-down list.

Step 15 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 16 Select the **Delete external user accounts on logout** checkbox to delete users who are not logged into a domain account after they log out.

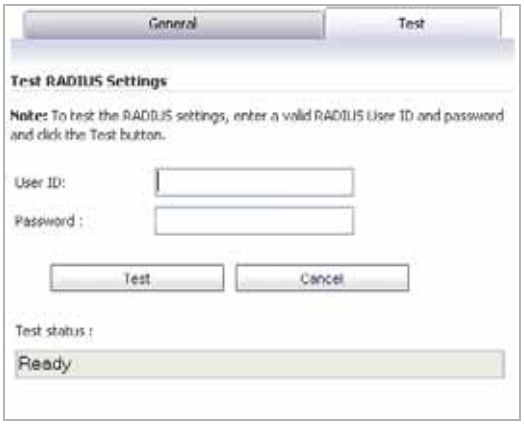
Step 17 Optionally select the **One-time passwords** checkbox to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

Step 18 If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

Step 19 Click **Add** to update the configuration. The domain will be added to the **Domain Settings** table.

Step 20 Click the configure button next to the RADIUS domain you added. The **Test** tab of the **Edit Domain** page displays.



Step 21 Enter your RADIUS user ID in the **User ID** field and your RADIUS password in the **Password** field.

Step 22 Click **Test**. SonicWALL SSL VPN will connect to your RADIUS server.

Step 23 If you receive the message **Server not responding**, check your user ID and password and click the **General** tab to verify your RADIUS settings. Try running the test again.

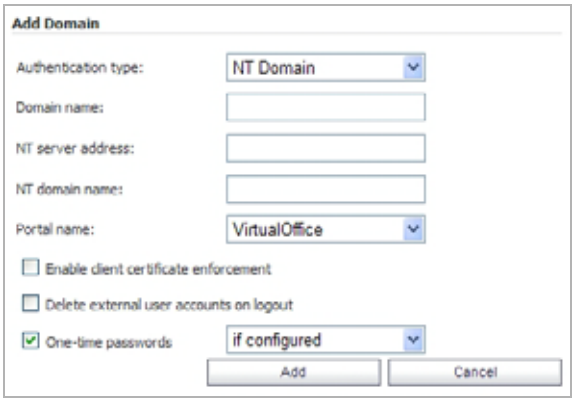
Note The SonicWALL SSL-VPN appliance will attempt to authenticate against the specified RADIUS server using PAP authentication. It is generally required that the RADIUS server be configured to accept RADIUS client connections from the SonicWALL SSL-VPN appliance. Typically, these connections will appear to come from the SonicWALL SSL-VPN's X0 interface IP address. Refer to your RADIUS server documentation for configuration instructions.

Adding a Domain with NT Domain Authentication

To configure NT Domain authentication, perform the following steps:

Step 1 On the **Portals > Domains** page, click **Add Domain** to display the **Add Domain** dialog box.

Step 2 Select **NT Domain** from the **Authentication Type** menu. The NT Domain configuration fields will be displayed.



Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name selected by users when they authenticate to the SonicWALL SSL-VPN appliance portal. It may be the same value as the **NT Domain Name**.

Step 4 Enter the IP address or host and domain name of the server in the **NT Server Address** field.

Step 5 Enter the NT authentication domain in the **NT Domain Name** field. This is the domain name configured on the Windows authentication server for network authentication.

Step 6 Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

Step 7 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 8 Select the **Delete external user accounts on logout** checkbox to delete users who are not logged into a domain account after they log out.

Step 9 Optionally select the **One-time passwords** checkbox to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

Step 10 If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

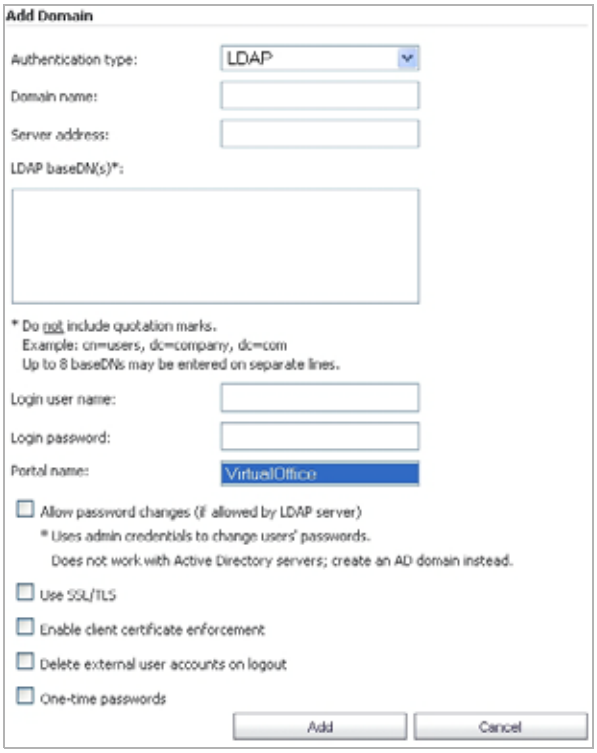
Step 11 Click **Add** to update the configuration. Once the domain has been added, the domain will be added to the **Domain Settings** table.

Adding a Domain with LDAP Authentication

To configure LDAP authentication, perform the following steps:

Step 1 Click **Add Domain** to display the **Add New Domain** dialog box.

Step 2 Select LDAP from the **Authentication Type** menu. The LDAP domain configuration fields is displayed.



Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL-VPN appliance user portal. It can be the same value as the **Server Address** field.

Step 4 Enter the IP address or domain name of the server in the **Server Address** field.

Step 5 Enter the search base for LDAP queries in the **LDAP baseDN** field. An example of a search base string is **CN=Users,DC=yourdomain,DC=com**.

Tip It is possible for multiple OUs to be configured for a single domain by entering each OU on a separate line in the **LDAP baseDN** field. In addition, any sub-OUs will be automatically included when parents are added to this field.

Note Do not include quotes (“”) in the **LDAP BaseDN** field.

Step 6 Enter the common name of a user that has been delegated control of the container that user will be in along with the corresponding password in the **Login Username** and **Login Password** fields.

Note When entering **Login Username** and **Login Password**, remember that the SSL-VPN appliance binds to the LDAP tree with these credentials and users can log in with their sAMAccountName.

Step 7 Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

Step 8 Optionally select the **Allow password changes (if allowed by LDAP server)** checkbox. This option, if allowed by your LDAP server, will enable users to change their LDAP password during an SSL VPN session.

Step 9 Optionally select the **Use SSL/TLS** checkbox. This option allows for the SSL/TLS encryption to be used for LDAP password exchanges. This option is disabled by default as not all LDAP servers are configured for SSL/TLS.

Step 10 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user’s account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 11 Optionally select the **One-time passwords** checkbox to enable the One Time Password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the **LDAP e-mail attribute** drop-down list will appear, in which you can select **mail**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your LDAP server is configured to store email addresses using the “mail” attribute, select **mail**.
- **mobile** or **pager** - If your AD server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, however, SMS addresses can.
- **userPrincipalName** - If your LDAP server is configured to store email addresses using the “userPrincipalName” attribute, select **userPrincipalName**.
- **custom** - If your LDAP server is configured to store email addresses using a custom attribute, select **custom**. If the specified attribute cannot be found for a user, the email address assigned in the individual user policy settings will be used. If you select **custom**, the **Custom attribute** field will appear. Type the custom attribute that your LDAP server uses to store email addresses. If the specified attribute cannot be found for a user, the email address will be taken from their individual policy settings.

If **using domain name** is selected in the **One-time passwords** drop-down list, the **E-mail domain** field will appear instead of the **LDAP e-mail attribute** drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

Step 12 Click **Add** to update the configuration and add the domain to the **Domains Settings** table.

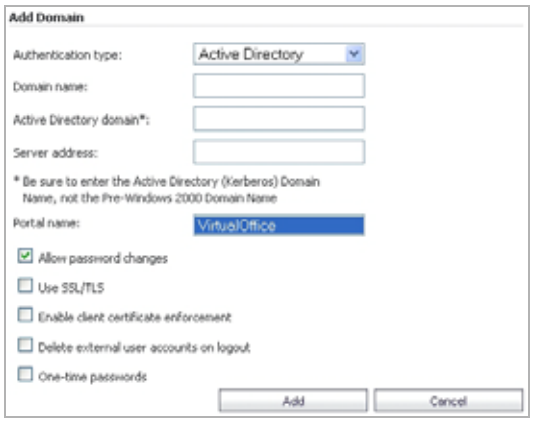
Adding a Domain with Active Directory Authentication

To configure Windows Active Directory authentication, perform the following steps:

Step 1 Click **Add Domain** to display the **Add Domain** dialog box.

Note *Of all types of authentication, Active Directory authentication is most sensitive to clock skew, or variances in time between the SonicWALL SSL-VPN appliance and the Active Directory server against which it is authenticating. If you are unable to authenticate using Active Directory, refer to “Active Directory Troubleshooting” section on page 132.*

Step 2 Select **Active Directory** from the **Authentication type** drop-down list. The Active Directory configuration fields will be displayed.



Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL-VPN appliance portal. It can be the same value as the **Server Address** field or the **Active Directory Domain** field, depending on your network configuration.

Step 4 Enter the Active Directory domain name in the **Active Directory Domain** field.

Step 5 Enter the IP address or host and domain name of the Active Directory server in the **Server Address** field.

Step 6 Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

Step 7 Optionally select the **Allow Password Changes Checkbox**. Enabling this feature allows a user to change their password through the Virtual Office portal by selecting the **Options** button on the top of the portal page. User must submit their old password, along with a new password and a re-verification of the newly selected password.

Step 8 Optionally select the **Use SSL/TLS** checkbox. This option allows for the needed SSL/TLS encryption to be used for Active Directory password exchanges. This checkbox should be enabled when setting up a domain using Active Directory authentication.

Step 9 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 10 Select the **Delete external user accounts on logout** checkbox to delete users who are not logged into a domain account after they log out.

Step 11 Optionally, select the **One-time passwords** checkbox to enable the One Time Password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

Step 12 If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the Active Directory **AD e-mail attribute** drop-down list will appear, in which you can select **mail**, **mobile**, **pager**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your AD server is configured to store email addresses using the "mail" attribute, select **mail**.
- **mobile** or **pager** - If your AD server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, however, SMS addresses can.
- **userPrincipalName** - If your AD server is configured to store email addresses using the "userPrincipalName" attribute, select **userPrincipalName**.

- **custom** - If your AD server is configured to store email addresses using a custom attribute, select **custom**. If the specified attribute cannot be found for a user, the email address assigned in the individual user policy settings will be used. If you select **custom**, the **Custom attribute** field will appear. Type the custom attribute that your AD server uses to store email addresses. If the specified attribute cannot be found for a user, the email address will be taken from their individual policy settings.

If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

Step 13 Click **Add** to update the configuration. Once the domain has been added, the domain will be added to the **Domain Settings** table.

Active Directory Troubleshooting

If your users are unable to connect using Active Directory, verify the following configurations:

- The time settings on the Active Directory server and the SonicWALL SSL-VPN appliance must be synchronized. Kerberos authentication, used by Active Directory to authenticate clients, permits a maximum 15-minute time difference between the Windows server and the client (the SonicWALL SSL-VPN appliance). The easiest way to solve this issue is to configure Network Time Protocol on the **System > Time** page of the SonicWALL SSL VPN Web-based management interface and check that the Active Directory server has the correct time settings.
- Confirm that your Windows server is configured for Active Directory authentication. If you are using Window NT4.0 server, then your server only supports NT Domain authentication. Typically, Windows 2000 and 2003 servers are also configured for NT Domain authentication to support legacy Windows clients.

Viewing the Domain Settings Table

All of the configured domains are listed in the **Domain Settings** table in the **Portals > Domains** window. The domains are listed in the order in which they were created.

Removing a Domain

To delete a domain, perform the following steps:

Step 1 Navigate to **Portals > Domains**.

Step 2 In the **Domain Settings** table, click the delete icon in the same row as the domain that you wish to delete.

Step 3 Click **OK** in the confirmation dialog box.

Once the SonicWALL SSL-VPN appliance has been updated, the deleted domain will no longer be displayed in the **Domain Settings** table.

Note The default LocalDomain domain cannot be deleted.

Configuring Two-Factor Authentication

Two-factor authentication is an authentication method that requires two independent pieces of information to establish identity and privileges. Two-factor authentication is stronger and more rigorous than traditional password authentication that only requires one factor (the user's password).

For more information on how two-factor authentication works see "Two-Factor Authentication Overview" section on page 27.

SonicWALL's implementation of two-factor authentication partners with two of the leaders in advanced user authentication: RSA and VASCO. If you are using RSA, you must have the RSA Authentication Manager and RSA SecurID tokens. If you are using VASCO, you must have the VASCO VACMAN Middleware and Digipass tokens.

To configure two-factor authentication, you must first configure a RADIUS domain. For information see "Adding a Domain with RADIUS Authentication" section on page 124.

The following sections describe how to configure the supported third-party authentication servers:

- "Configuring the RSA Authentication Manager" section on page 133
- "Configuring the VASCO VACMAN Middleware" section on page 138

Configuring the RSA Authentication Manager

(RSA is supported only on SonicWALL SSL-VPN models 2000 and higher.) The following sections describe how to configure the RSA Authentication Manager version 6.1 to perform two-factor authentication with your SonicWALL SSL-VPN appliance:

- "Adding an Agent Host Record for the SonicWALL SSL-VPN Appliance" section on page 133
- "Adding the SonicWALL SSL-VPN as a RADIUS Client" section on page 134
- "Setting the Time and Date" section on page 135
- "Importing Tokens and Adding Users" section on page 135

Note This configuration procedure is specific to RSA Authentication Manager version 6.1. If you are using a different version of RSA Authentication Manager, the procedure will be slightly different.

If you will be using VASCO instead of RSA, see "Configuring the VASCO VACMAN Middleware" on page 138.

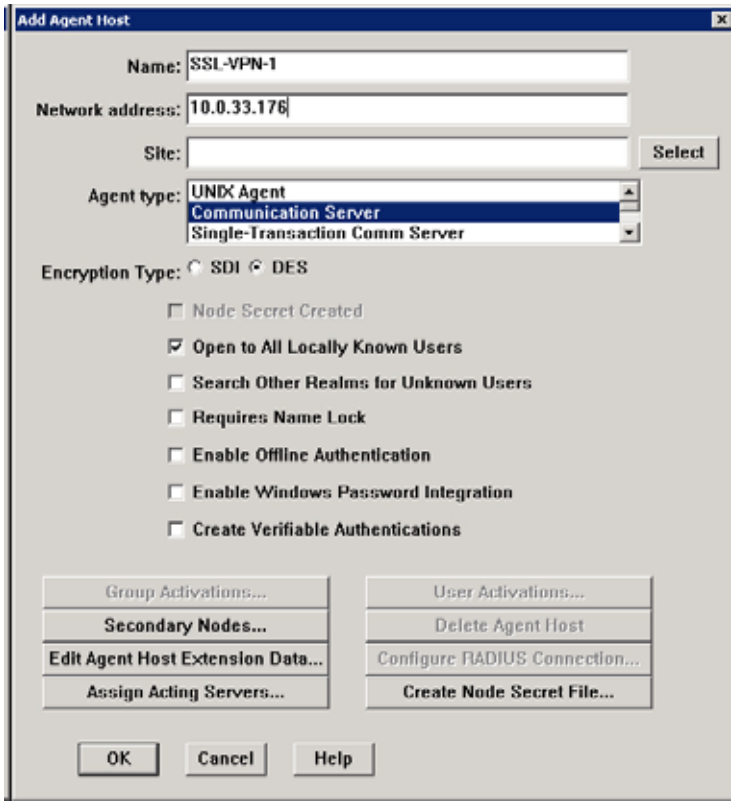
Adding an Agent Host Record for the SonicWALL SSL-VPN Appliance

To establish a connection between the SSL-VPN appliance and the RSA Authentication Manager, an Agent Host record must be added to the RSA Authentication Manager database. The Agent host record identifies the SSL-VPN appliance within its database and contains information about communication and encryption.

To create the Agent Host record for the SSL-VPN appliance, perform the following steps:

Step 1 Launch the RSA Authentication Manager.

Step 2 On the **Agent Host** menu, select **Add Agent Host**. The **Add Agent Host** window displays.



Step 3 Enter a hostname for the SSL-VPN appliance in the **Name** field.

Step 4 Enter the IP address of the SSL-VPN appliance in the **Network address** field.

Step 5 Select **Communication Server** in the **Agent type** window.

Step 6 By default, the **Enable Offline Authentication** and **Enable Windows Password Integration** options are enabled. SonicWALL recommends disabling all of these options except for **Open to All Locally Known Users**.

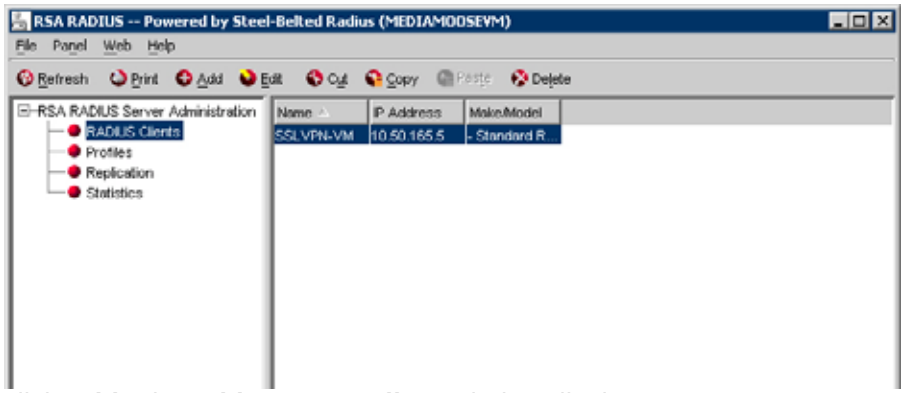
Step 7 Click **OK**.

Adding the SonicWALL SSL-VPN as a RADIUS Client

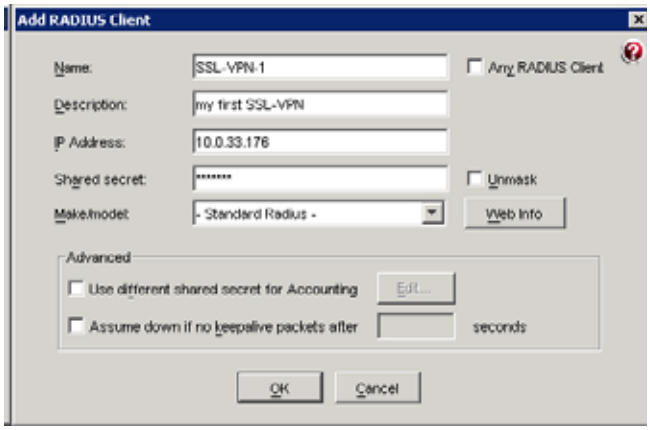
After you have created the Agent Host record, you must add the SonicWALL SSL-VPN to the RSA Authentication Manager as a RADIUS client. To do so, perform the following steps:

Step 1 In RSA Authentication Manager, go to the **RADIUS** menu and select **Manage RADIUS Server**. The **RSA RADIUS Manager** displays.

Step 2 Expand the **RSA RADIUS Server Administration** tree and select **RADIUS Clients**.



Step 3 Click **Add**. The **Add RADIUS Client** window displays.



Step 4 Enter a descriptive name for the SSL-VPN appliance.

Step 5 Enter the IP address of the SSL-VPN in the **IP Address** field.

Step 6 Enter the shared secret that is configured on the SSL-VPN in the **Shared secret** field.

Step 7 Click **OK** and close the RSA RADIUS Manager.

Setting the Time and Date

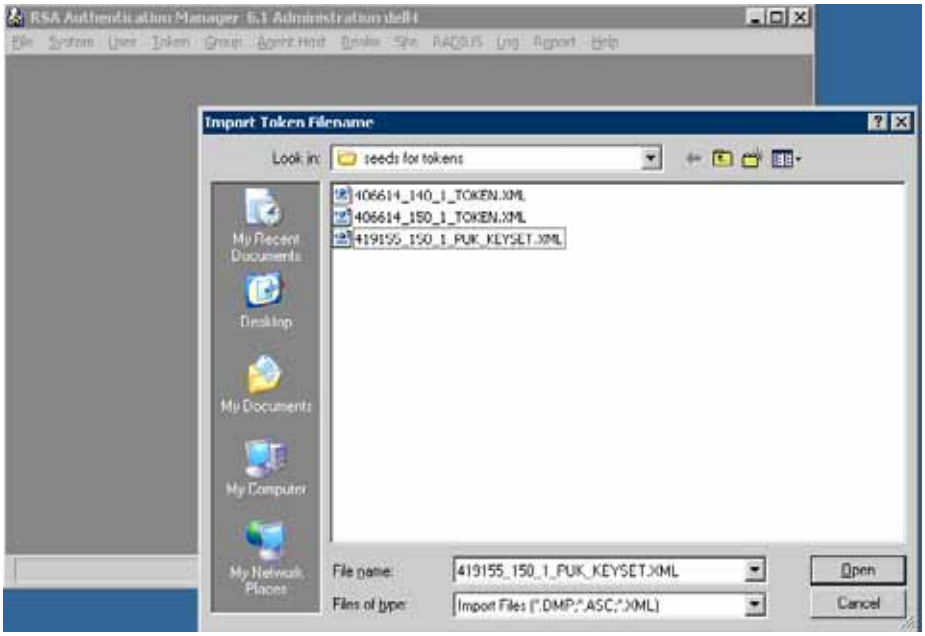
Because two-factor authentication depends on time synchronization, it is important that the internal clocks for the RSA Authentication Manager and the SSL-VPN appliance are set correctly.

Importing Tokens and Adding Users

After you have configured the RSA Authentication Manager to communicate with the SonicWALL SSL-VPN appliance, you must import tokens and add users to the RSA Authentication Manager.

To import tokens and add users, perform the following steps:

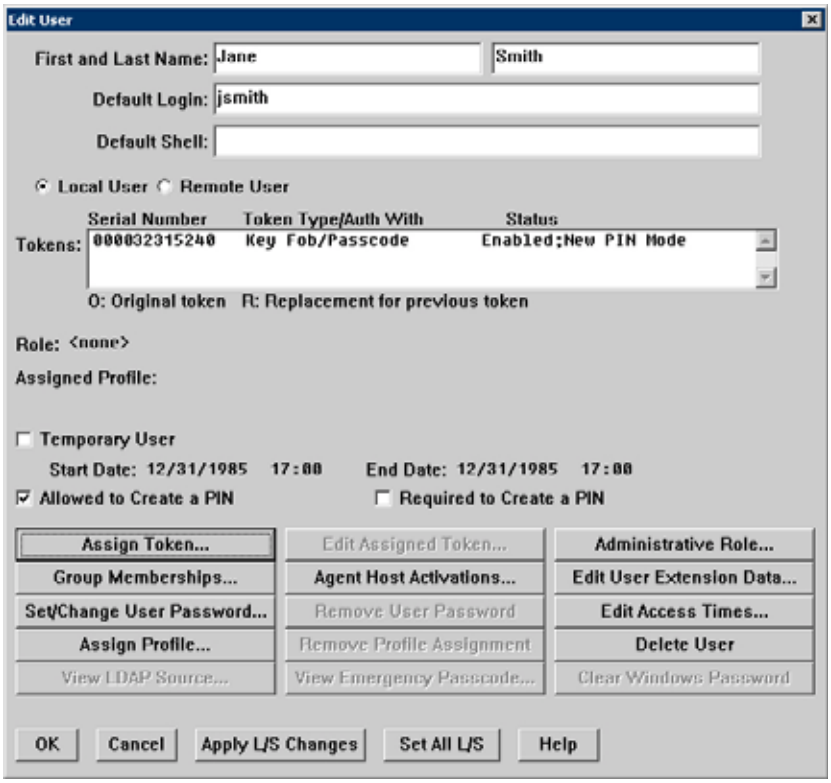
Step 1 To import the token file, select **Token > Import Tokens**.



Step 2 When you purchase RSA SecurID tokens, they come with an XML file that contains information on the tokens. Navigate to the token XML file and click **Open**. The token file is imported.

Step 3 The **Import Status** window displays information on the number of tokens imported to the RSA Authentication Manager.

Step 4 To create a user on the RSA Authentication Manager, click on **User > Add user**.

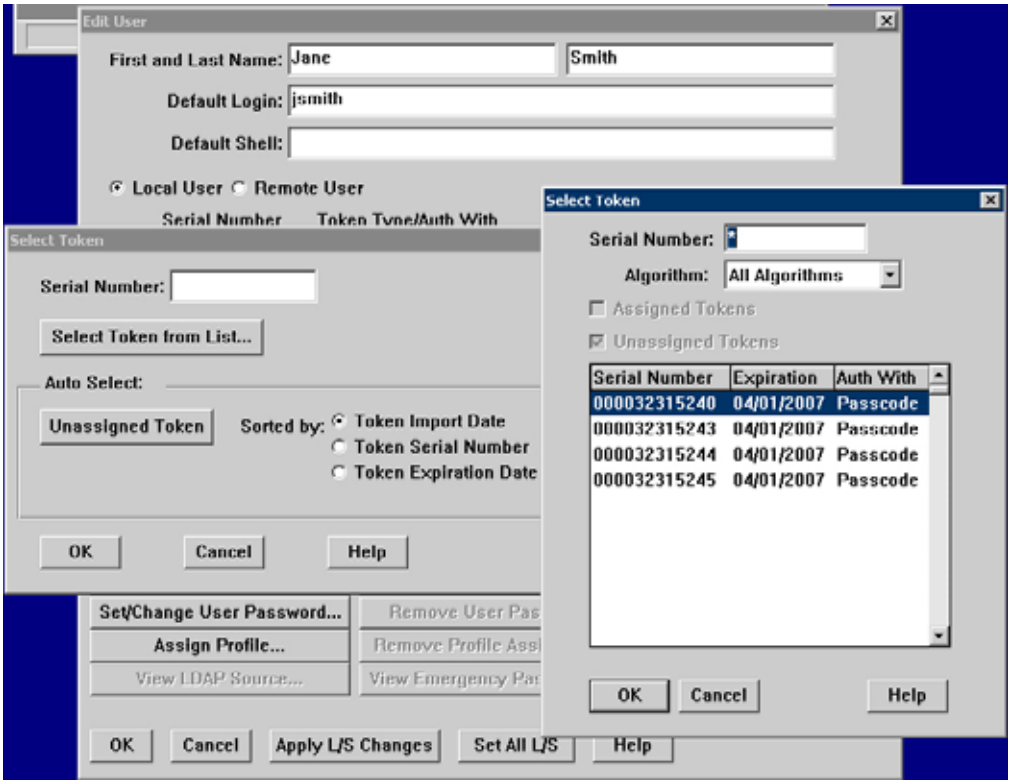


Step 5 Enter the user's **First and Last Name**.

Step 6 Enter the user's username in the **Default Login** field.

Step 7 Select either **Allowed to Create a PIN** or **Required to Create a PIN**. **Allowed to Create a PIN** gives users the option of either creating their own PIN or having the system generate a random PIN. **Required to Create a PIN** requires the user to create a PIN.

Step 8 To assign a token to the user, click on the **Assign Token** button. Click **Yes** on the confirmation window that displays. The **Select Token** window displays.



Step 9 You can either manually select the token or automatically assign the token:

- To manually select the token for the user, click **Select Token from List**. In the window that displays, select the serial number for the token and click **OK**.
- To automatically assign the token, you can optionally select the method by which to sort the token: the token's import date, serial number, or expiration date. Then click the **Unassigned Token** button and the RSA Authentication Manager assigns a token to the user. Click **OK**.

Step 10 Click **OK** in the **Edit User** window. The user is added to the RSA Authentication Manager.

Step 11 Give the user their RSA SecurID Authenticator and instructions on how to log in, create a PIN, and user the RSA SecurID Authenticator. See the *SonicWALL SSL VPN User Guide* for more information.

Configuring the VASCO VACMAN Middleware

The following sections describe how to configure two-factor authentication using VASCO's VACMAN Middleware Administration version 2.3:

Note This configuration procedure is specific to VACMAN Middleware Administration version 2.3. If you are using a different version of VACMAN Middleware Administration, the procedure will be slightly different.

If you will be using RSA instead of VASCO, see "Configuring the RSA Authentication Manager" on page 133.

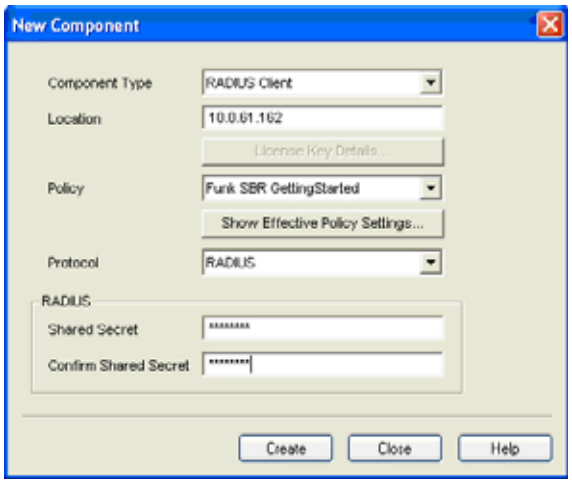
Adding the RADIUS Server to VACMAN Middleware

To create a connection between the Sonic wall SSL-VPN appliance and the VASCO server, you must create a component record for the external RADIUS server. VASCO servers do not have an internal RADIUS component, so they must use an external RADIUS server. To create a component record for the RADIUS server, perform the following steps:

Step 1 Launch the VACMAN Middleware Administration program.

Step 2 Expand the **VACMAN Middleware Administration** tree and the **VACMAN Server** tree.

Step 3 Right click on **RADIUS Servers** and click on **New RADIUS Server**.



Step 4 Enter the IP address of the RADIUS server in the **Location** field. Note that this is the IP address of the RADIUS server and *not* the SonicWALL SSL-VPN appliance.

Step 5 Select the appropriate policy in the **Policy** pull down menu.

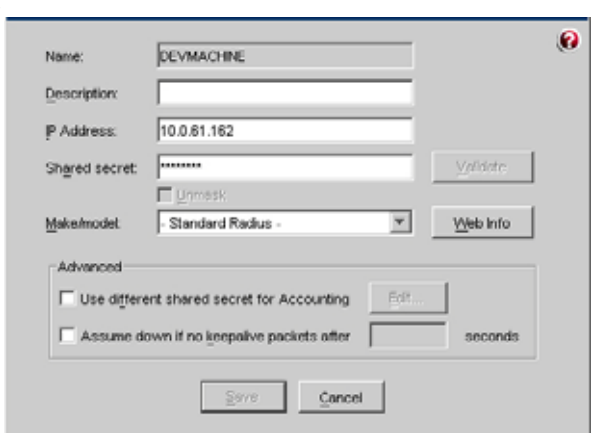
Step 6 Enter the RADIUS shared secret in the **Shared Secret** and **Confirm Shared Secret** fields.

Adding the SSL-VPN Appliance to VASCO

To add the SonicWALL SSL-VPN appliance to VACMAN Middleware Administrator as a RADIUS client, perform the following steps.

Step 1 Expand the **VACMAN Server** tree.

Step 2 Right-click on **RADIUS Clients** and click **New RADIUS Client**.



Step 3 Enter the **IP Address** of the SSL-VPN appliance.

Step 4 Enter the **Shared secret**.

Step 5 Click **Save**.

Setting the Time and Date

The DIGIPASS token is based on time synchronization. All tokens are created with their internal real-time clocks set to GMT. As such, it is important to set the date and time zone of the server running the VACMAN middleware to correctly so the GMT can be local derived correctly.

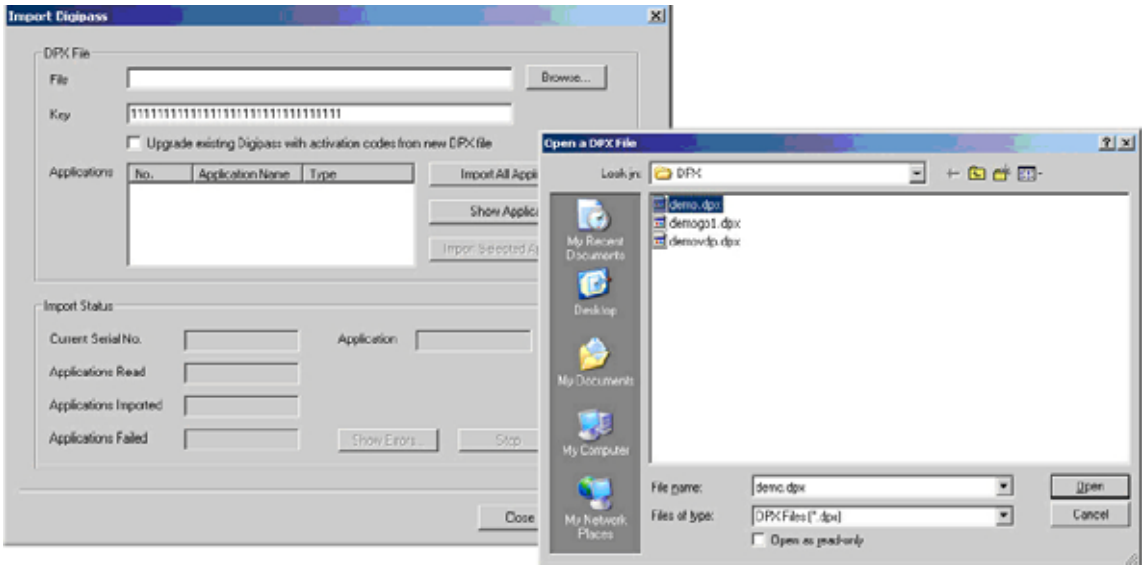
Importing Digipass Token Secret

Before Digipass tokens can be assigned to a user, their application records must be imported to the VACMAN middleware. To do this, perform the following steps.

Step 1 Right-click on the **Digipass** node under the **VACMAN server** tree.

Step 2 Click **Import Digipass**.

Step 3 Click **Browse**, navigate to the location of the Digipass import file, and click **Open**.



Step 4 Enter the Digipass import key in the **Key** field. The key is a 32-character hexadecimal number.

Step 5 Click **Import All Applications** to import all records in the file. Or to select the records to import, click **Show Applications**, select the records to import, and click **Import Selected Applications**.

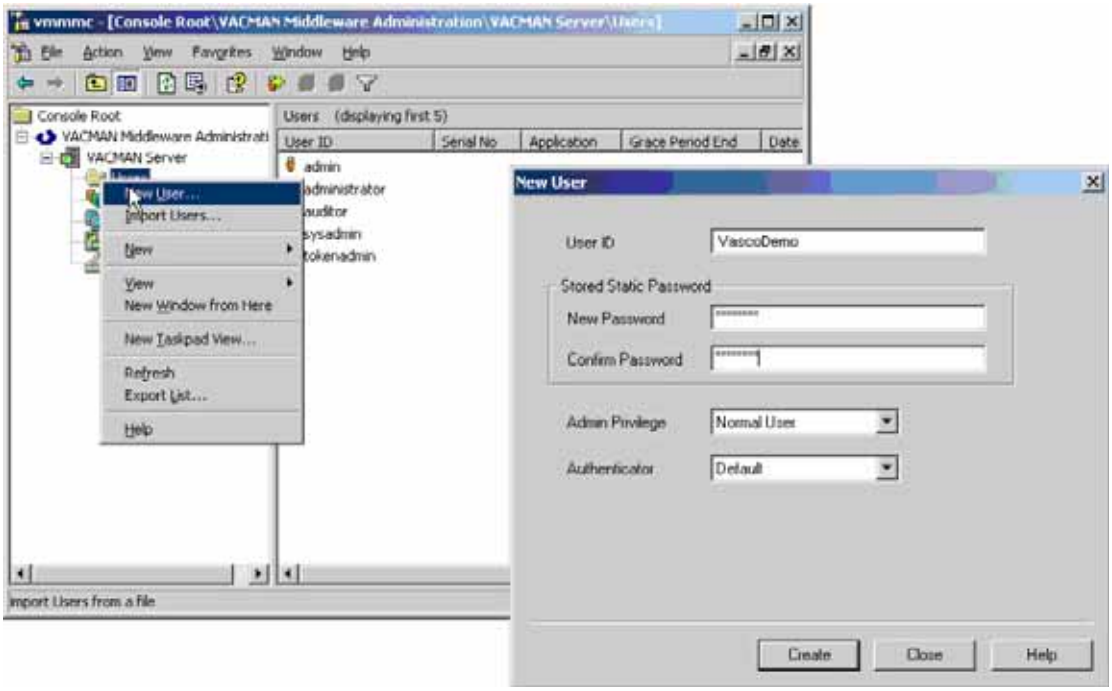
Step 6 The progress of the import procedure will be shown in the bottom **Import Status** section.

Creating Users

To add users to the VACMAN Middleware Administration, perform the following steps.

Step 1 Expand the **VACMAN Server** tree and right-click on **Users**.

Step 2 Click **New User**.



Step 3 Enter the username in the **User ID** field.

Step 4 Enter the user's password in the **New Password** and **Confirm Password** fields.

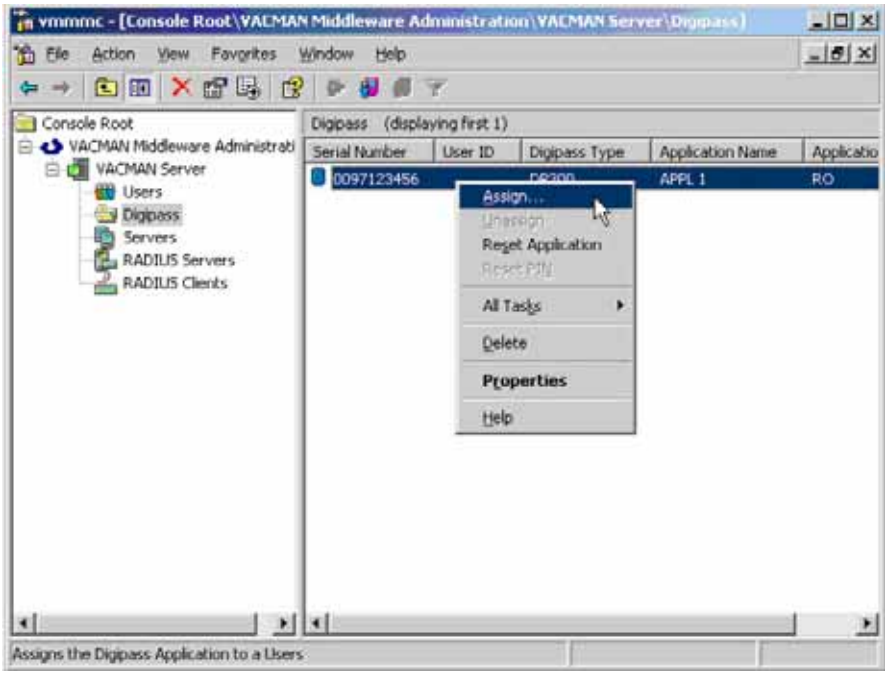
Step 5 Select the appropriate **Admin Privilege** and **Authenticator**.

Step 6 Click **Create**.

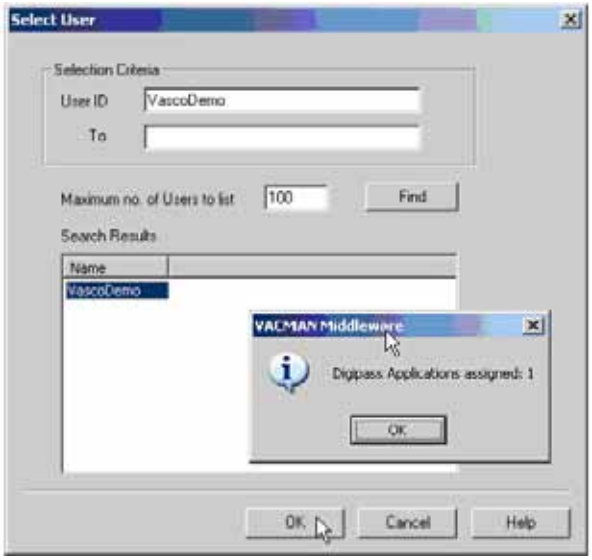
Assigning Digipass Tokens to Users

After you have imported the digipass tokens and created the users, you need to assign the Digipass tokens to the users. To do so, perform the following steps.

Step 1 Expand the **VACMAN Server** tree and click on **Digipass**.



Step 2 Right-click on the serial number of the Digipass token you want to assign and click **Assign**.

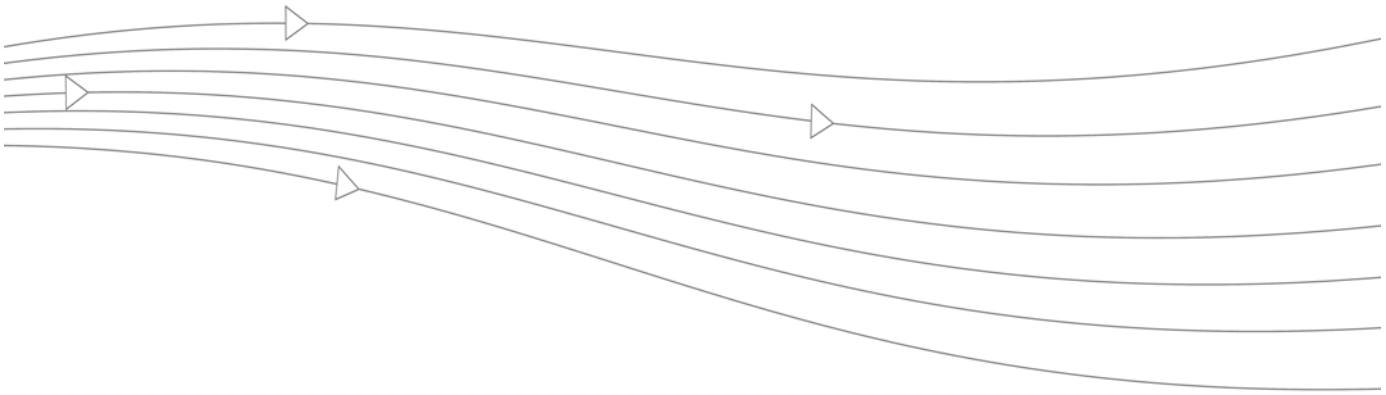


Step 3 Enter the username in the **User ID** field and click the **Find** button.

When the username is displayed in the **Search Results** window, select the username and click **OK** to assign the Digipass token.

Portals > Custom Logo

On SonicWALL SSL-VPN 2000 and 4000 appliances, beginning with the SSL VPN 2.5 release, portal logos are no longer configured globally from the **Portals > Custom Logo** page. Custom logos are uploaded on a per-portal basis from the **Logo** tab in the **Portal Logo Settings** dialogue. For information related to Custom Portal Logos on models 2000 and higher, refer to the "Adding a Custom Portal Logo" section on page 116.



Chapter 5: Services Configuration

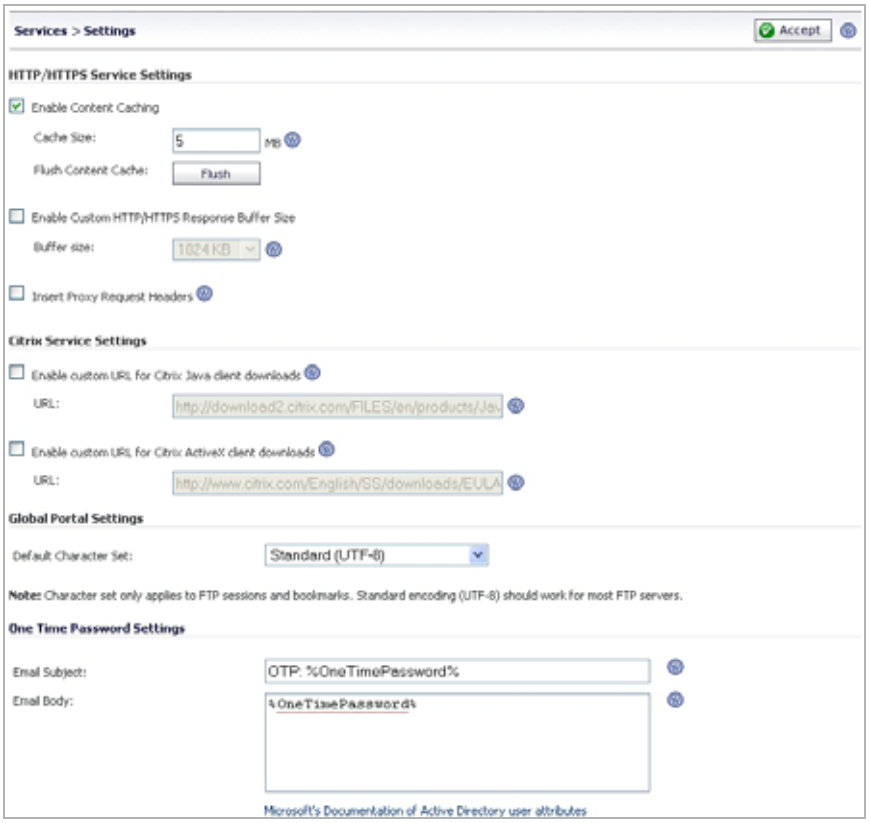
This chapter provides information and configuration tasks specific to the **Services** pages on the SonicWALL SSL VPN Web-based management interface, including configuring settings, bookmarks, and policies for various application layer services, such as HTTP/HTTPS, Citrix, RDP, and VNC.

This chapter contains the following sections:

Services > Settings

This section provides an overview of the **Services > Settings** page and a description of the configuration tasks available on this page.

The **Services > Settings** page allows the administrator to configure various settings related to HTTP/HTTPS, Citrix, Global Portal character sets, and one-time passwords.



HTTP/HTTPS Service Settings

Administrators can take the following steps to configure HTTP/HTTPS Service Settings:

Step 1 The **Enable Content Caching** checkbox is selected by default. Administrators may disable the checkbox if they choose to do so. However, changing the Enable Content Cache setting will restart SSL VPN Services, including the web server.

In the **Cache Size** field, define the size of the desired content cache. 5 MB is the default setting, but administrators may set any size in the valid range from two to 20 MB. Select the **Flush** button to flush the content cache.

Step 2 Select the **Enable Custom HTTP/HTTPS Response Buffer Size** checkbox, if you wish to establish a response buffer. Enabling this checkbox. Set the desired buffer size using the **Buffer size** drop-down menu. This limit is enforced for HTTP and HTTPS responses from the backend Web server for plain text, Flash, and Java applets. The default size of the buffer is 1024 KB.

Step 3 Enable the **Insert Proxy Request Headers** checkbox to insert these types of headers into the HTTP/HTTPS requests to the backend Web server. The following headers will be inserted:

- **X-Forwarded-For**: Specifies the client IP address of the original HTTP/HTTPS request.
- **X-Forwarded-Host**: Specifies the "Host" in the HTTP/HTTPS request from the client.
- **X-Forwarded-Server**: Specifies the host name of the SSL VPN proxy server.

Citrix Service Settings

Administrators can take the following steps to configure Citrix Service Settings:

Step 1 Select the **Enable custom URL for Citrix Java client downloads** checkbox if you want to use your own HTTP URL to download the Citrix Java client. Fill-in the custom URL in the **URL** field. If this option is not enabled, the default URL will be used.

Step 2 Select the **Enable custom URL for Citrix ActiveX client downloads** checkbox if you want to use your own HTTP URL to download the Citrix ActiveX client. Fill-in the custom URL in the **URL** field. If this option is not enabled, the default URL will be used.

Global Portal Settings

Step 1 Use the **Default Character Set** drop-down menu to set the language compatibility character set to be used with standard and non-standard FTP servers. The character set only applies to FTP sessions and bookmarks. Standard encoding (UTF-8), the default setting, should work for most FTP servers.

One Time Password Settings

The **One Time Password Settings** section allows administrators to configure settings relating to the creation and communication of one-time passwords. One-time passwords are dynamically generated strings of characters, numbers or a combination of both. For compatibility with mail services that allow a limited number of characters in the email subject (such as SMS), the administrator can customize the email subject to either include or exclude the one-time password. The email message body can also be configured in the same way. The administrator can also select the format (such as characters and numbers) for the password.

To configure the One Time Password email subject format, email body format, and change the default character types used when generating one time passwords, perform the following tasks:

Step 1 In the **Email Subject** field, type the desired text for the one-time password email subject. The default subject consists of **OTP** plus the actual one-time password (represented here with the parameter placeholder **%OneTimePassword%**).

Step 2 In the **Email Body** field, type the desired text for the one-time password email message body. The default message is simply the one-time password itself (represented here as **%OneTimePassword%**).

Variables can be used in the subject or body of a one-time password email:

- %**OneTimePassword**% - The user's one-time password. This should appear at least once in either the email subject or body.
- %**AD:mobile**% - The user's mobile phone as configured in Active Directory (AD).
- %**AD:**_____% - Any other Active Directory (AD) user attribute. See the Microsoft documentation link below the **Email Body** field for additional attributes.

Step 3 In the **One Time Password Format** drop-down list, select one of the following three options:

- **Characters** – Only alphabetic characters will be used when generating the one-time password.
- **Characters and Numbers** – Alphabetic characters and numbers will be used when generating the one-time password.
- **Numbers** – Only numbers will be used when generating the one-time password.

Step 4 Use the **One Time Password Length** fields to adjust the range of characters allowed for one-time passwords.

Step 5 Click the **Accept** button in the upper right corner of the **Services > Settings** page to save your changes.

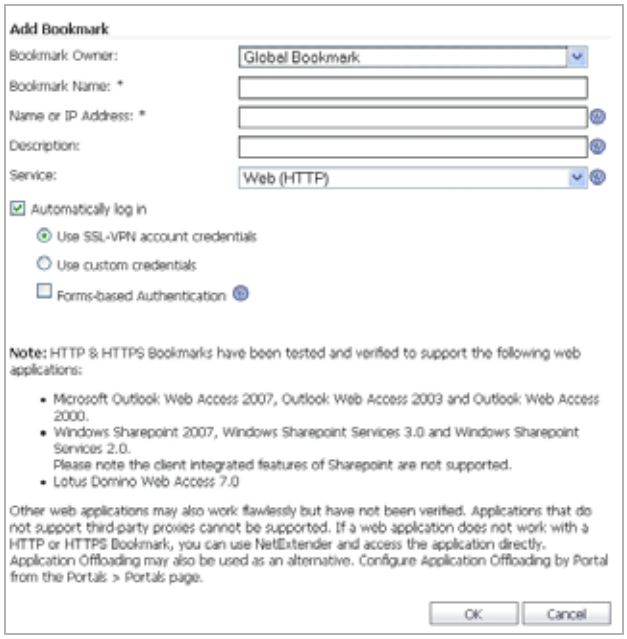
For more information about the One Time Passwords feature, refer to the "One Time Password Overview" section on page 28.

Services > Bookmarks

The **Services > Bookmarks** page within the Web-based management interface provides a single interface for viewing bookmarks and access to configure bookmarks for users and groups.

Adding or Editing a Bookmark

To add a bookmark, navigate to the **Services > Bookmarks** screen within the management interface and select the **Add Bookmark...** button. The **Add Bookmark** dialog box opens in a separate window.



Complete the following steps to add a service bookmark:

Step 1 Use the **Bookmark Owner** drop-down menu to select whether the bookmark is owned as a **Global Bookmark**, a **Local Domain** group bookmark, or a bookmark assigned to an individual **User**.

Step 2 Fill-in the Bookmark Name field with a friendly name for the service bookmark.

Step 3 Fill-in the Name or IP Address field with hostname, IP address, or IPv6 address for the desired bookmark. IPv6 addresses should begin with “[“ and end with “]”.

Note IPv6 is not supported by File Shares.

Some services can run on non-standard ports, and some expect a path when connecting. Depending on the choice in the Service field, format the **Name or IP Address** field like one of the examples shown in the following table.

Service Type	Format	Example for Name or IP Address Field
RDP - ActiveX	IP Address	10.20.30.4
RDP - Java	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
VNC	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (mapped to session)	10.20.30.4:5901 (mapped to session 1)
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
	Note: Do not use session or display number instead of port.	**Note**: Do not use 10.20.30.4:1 **Tip**: For a bookmark to a Linux server, see the Tip below this table.
FTP	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
Telnet	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
SSHv1	IP Address	10.20.30.4
SSHv2	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC

Service Type	Format	Example for Name or IP Address Field
HTTP	URL	www.sonicwall.com
HTTPS	IP Address of URL	204.212.170.11
	IPv6 Address	2008::1:2:3:4
	URL:Path or File	www.sonicwall.com/index.html
	IP:Path or File	204.212.170.11/folder/
	URL:Port	www.sonicwall.com:8080
	IP:Port	204.212.170.11:8080 or [2008::1:2:3:4]:8080
	URL:Port:Path or File	www.sonicwall.com:8080/folder/index.html
	IP:Port:Path or File	204.212.170.11:8080/index.html
File Shares	Host\Folder\	server-3\sharedfolder\
	Host\File	server-3\inventory.xls
	FQDN\Folder	server-3.company.net\sharedfolder\
	FQDN\File	server-3company.net\inventory.xls
	IP\Folder\	10.20.30.4\sharedfolder\
	IP\File	10.20.30.4\status.doc
		Note: Use backslashes even on Linux or Mac computers; these use the Windows API for file sharing.
Citrix	IP Address	172.55.44.3
(Citrix Web Interface)	IPv6 Address	2008::1:2:3:4
	IP:Port	172.55.44.3:8080 or [2008::1:2:3:4]:8080
	IP:Path or File	172.55.44.3/folder/file.html
	IP:Port:Path or File	172.55.44.3:8080/report.pdf
	FQDN	www.citrixhost.company.net
	URL:Path or File	www.citrixhost.net/folder/
	URL:Port	www.citrixhost.company.com:8080
	URL:Port:Path or File	www.citrixhost.com:8080/folder/index.html
	Note: *Port* refers to the HTTP(S) port of Citrix Web Interface, not to the Citrix ICA client port.	

Tip When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

Step 4 Use the Service drop-down menu to select the desired bookmark service. Use the following information for the chosen service to complete the building of the bookmark.

Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)

Note If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark.

  Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session.
- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Optionally, enter the local path for this application in the **Application and Path** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select the **Login as console/admin session** checkbox to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Select the **Enable wake-on-LAN** checkbox to enable waking up a computer over the network connection. Selecting this checkbox causes the following new fields to be displayed:
  - **MAC/Ethernet Address** – Enter one or more MAC addresses, separated by spaces, of target hosts to wake.
  - **Wait time for boot-up (seconds)** – Enter the number of seconds to wait for the target host to fully boot up before cancelling the WOL operation.
  - **Send WOL packet to host name or IP address** – To send the WOL packet to the hostname or IP of this bookmark, select the **Send WOL packet to host name or IP address** checkbox, which can be applied in tandem with a MAC address of another machine to wake.
- For **RDP - ActiveX** on Windows clients, expand **Show client redirect options** and select any of the redirect checkboxes **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, or **Redirect SmartCards** to redirect those devices on the local network for use in this bookmark session. You can hover your mouse pointer over these options to display tooltips that indicate requirements for certain actions.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.
- For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advance Windows options** and select the checkboxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

  Select the checkboxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.
Remote Application monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.

- For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces. Note that the RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. The **Enable plugin DLLs** option is not available for RDP - Java. See "Enabling Plugin DLLs" section on page 221.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Virtual Network Computing (VNC)

- In the **Encoding** drop-down menu, select the desired encoding transfer format.
- Optionally, if available, use the **Compression Level** drop-down menu to select the desired compression level for data.
- Optionally, if available, select the JPEG image file quality level using the **JPEG Image Quality** drop-down menu.
- In the **Cursor Shape Updates** drop-down menu, select to either Enable, Disable, or Ignore these updates.
- Enable or disable the **CopyRect** function using the associated checkbox.
- Enable or disable the use of only **Restricted Colors** by using the associated checkbox.
- Enable or disable the ability to **reverse control of mouse buttons two and three** using the associated checkbox.
- Enable the **View Only** checkbox to control to prevent taking control over VNC.
- Enable the **Share Desktop** checkbox to allow desktop view to be shared over VNC.

Citrix Portal (Citrix)

- Optionally, select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal. HTTPS mode is used to encrypt communication between the SSL VPN device and the Citrix server using the SSL protocol.
- Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client or XenApp plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this checkbox leverages this portability.

Web (HTTP)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Secure Web (HTTPS)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

File Shares (CIFS)

- To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** checkbox.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

  When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SonicWALL SSL-VPN is not a domain member and will not be able to connect to the DFS shares.

  DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

File Transfer Protocol (FTP)

- Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Telnet

- No additional fields

Secure Shell version 1 (SSHv1)

- No additional fields

Secure Shell version 2 (SSHv2)

- Optionally select the **Automatically accept host key** checkbox.
- If using an SSHv2 server without authentication, such as a SonicWALL firewall, you can select the **Bypass username** checkbox.

Step 5 Click **OK** to update the configuration. Once the configuration has been updated, the new user bookmark will be displayed in the **Services >Bookmarks** window.

Editing a Bookmark

To edit a service bookmark, navigate to the **Services > Bookmarks** screen. Click on the **pencil icon** in the **Configure** column. A new **Edit Bookmark** window will open with the bookmark's current configuration. Make all desired adjustments and select **OK**. The edited bookmark will still display in the **Services > Bookmarks** window.

Deleting a Bookmark

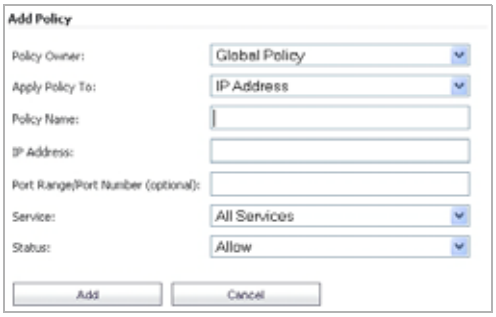
To delete a configured bookmark, navigate to the **Services > Bookmarks** screen. Click on the "**X**" icon in the **Configure** column. A dialog box will open and ask if you are sure you want to delete the specified bookmark. Click **OK** to delete the bookmark. The bookmark will no longer appear in the Services > Bookmarks screen.

Services > Policies

The **Services > Policies** page within the Web-based management interface provides a single interface for viewing service policies and access to configure policies for users and groups.

Adding or Editing a Policy

To add a policy, navigate to the **Services > Policies** screen within the management interface and select the **Add Policy...** button. The **Add Policy** dialog box opens in a separate window.



Administrators can follow the following steps to add a service policy:

Step 1 Use the **Policy Owner** drop-down menu to select whether the policy is owned as a **Global Policy**, a **Local Domain** group policy, or a policy assigned to an individual **User**.

Step 2 In the **Apply Policy To** drop-down menu, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. On SonicWALL SSL-VPN models 2000 and higher, you can also select an individual IPv6 host, a range of IPv6 addresses, or all IPv6 addresses. The **Add Policy** dialog box changes depending on what type of object you select in the **Apply Policy To** drop-down list.

Note These SonicWALL SSL VPN policies apply to the destination address(es) of the SonicWALL SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SonicWALL SSL VPN gateway with a policy created on the **Policies** tab. However, it is possible to control source logins by IP address with a login policy created on the user's **Login Policies** tab. For more information, refer to "Configuring Login Policies" section on page 224.

Step 3 Follow the appropriate step below depending on your selection in the **Apply Policy To** menu.

- **IP Address** - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IP Address" section on page 211.

- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally, enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IP Address Range" section on page 211.
- **All Addresses** - If your policy applies to all IPv4 addresses, you do not need to enter any IP address information. See "Adding a Policy for All Addresses" section on page 212.
- **Network Object -** If your policy applies to a predefined network object, select the name of the object from the **Network Object** drop-down list. A port or port range can be specified when defining a Network Object. See "Configuring Network Objects" section on page 101
- **Server Path** - If your policy applies to a server path, select one of the following radio buttons in the **Resource** field:
  - **Share (Server path)** - When you select this option, type the path into the **Server Path** field.
  - **Network (Domain list)**
  - **Servers (Computer list)**

  See "Setting File Shares Access Policies" section on page 212.
- **URL Object** - If your policy applies to a predefined URL object, type the URL into the **URL** field. See "Adding a Policy for a URL Object" section on page 213.
- **IPv6 Address** - On SonicWALL SSL-VPN models 2000 and higher, if your policy applies to a specific host, enter the IPv6 address of the local host machine in the **IPv6 Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IPv6 Address" section on page 215.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IPv6 Address" section on page 215.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See "Adding a Policy for All IPv6 Addresses" section on page 215.

Step 4 Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

Step 5 Select **ALLOW** or **DENY** from the **Status** drop-down list to either allow or deny SonicWALL SSL VPN connections for the specified service and host machine.

Tip When using Citrix bookmarks, in order to restrict proxy access to a host, a DENY rule must be configured for both Citrix and HTTP services.

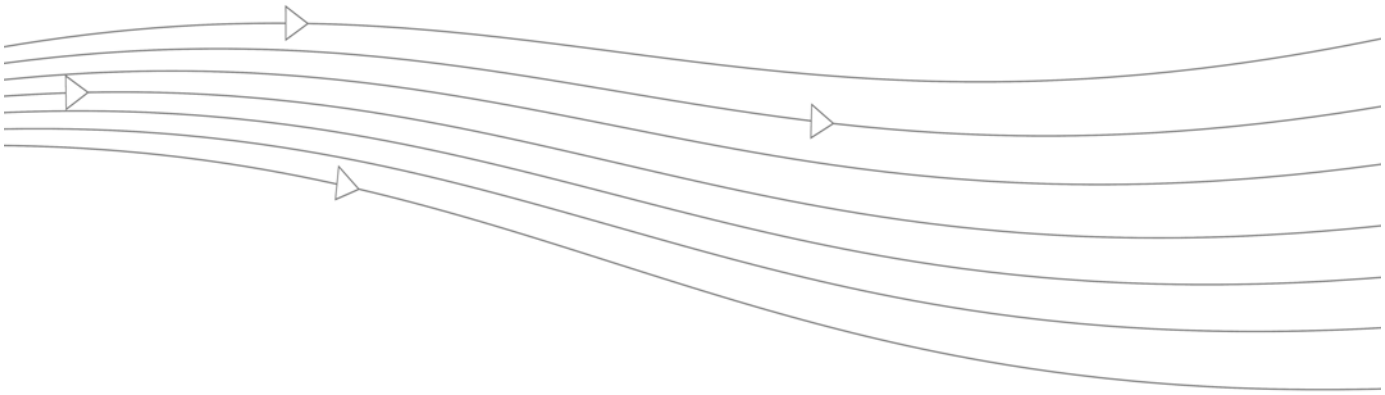
Step 6 Click **Add** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Services > Policies** window.

Editing a Policy

To edit a service-related policy, navigate to the **Services > Policies** screen. Click on the **pencil icon** in the **Configure** column. A new **Edit Policy** window will open with the bookmark's current configuration. Make all desired adjustments and select **OK**. The edited bookmark will still display in the **Services > Policies** window.

Deleting a Policy

To delete a configured policy, navigate to the **Services > Policies** screen. Click on the "**X**" icon in the **Configure** column. A dialog box will open and ask if you are sure you want to delete the specified policy. Click **OK** to delete the policy. The policy will no longer appear in the **Services > Policies** screen.



Chapter 6: NetExtender Configuration

This chapter provides information and configuration tasks specific to the NetExtender pages on the SonicWALL SSL VPN Web-based management interface.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients to have seamless access to resources on your local network.

Users can access NetExtender two ways: Using the Net Extender button on the SonicWALL SSL VPN user portal, or by using the NetExtender standalone client, which is installed by clicking on the NetExtender button in the SonicWALL SSL VPN Web-based management interface. The NetExtender standalone client application can be accessed directly from the Windows Start menu, from the Application folder or dock on Mac systems, and by pathname or from the shortcut bar on Linux systems.

The standalone NetExtender Mobile client is available for devices running Windows Mobile 5 PocketPC and Windows Mobile 6 Professional/Classic.

SonicWALL SSL-VPN supports client certificates in both the standalone Windows NetExtender client and the NetExtender Mobile client.

NetExtender supports IPv6 client connections from Windows systems running Windows Vista or newer, and from Linux clients. An IPv6 address pool for NetExtender is optional, while an IPv4 address pool is necessary. IPv6 is only supported on SonicWALL SSL-VPN models 2000 and higher.

For more information on NetExtender concepts, see "NetExtender Overview" section on page 17. For information about using or installing the NetExtender or NetExtender Mobile clients, see the latest *SonicOS SSL-VPN User's Guide*, available on the Secure Remote Access pages of the SonicWALL Support Web site at:
http://www.sonicwall.com/us/Support.html

This chapter contains the following sections:

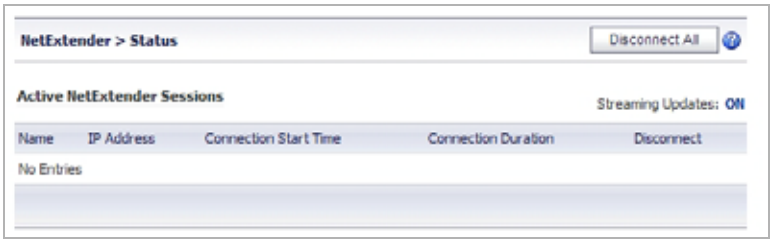
NetExtender > Status

This section provides an overview of the **NetExtender > Status** page and a description of the configuration tasks available on this page.

NetExtender > Status Overview

The **NetExtender > Status** page allows the administrator to view active NetExtender sessions, including the name, IP address, login time, length of time logged in and logout time.

Figure 23 NetExtender > Status



Viewing NetExtender Status

The **NetExtender > Status** page allows the administrator to view active NetExtender sessions, including the name, IP address, login time, length of time logged in and administrative logout control. Table 11 provides a description of the status items.

Table 11 NetExtender Status

Status Item	Description
Name	The user name.
IP Address	The IP address of the workstation on which the user is logged into.
Login Time	The time when the user first established connection with the SonicWALL SSL-VPN appliance expressed as day, date, and time (HH:MM:SS).
Logged in	The amount of time since the user first established connection with the SonicWALL SSL-VPN appliance expressed as number of days and time (HH:MM:SS).
Logout	Provides the administrator the ability to logout a NetExtender session.

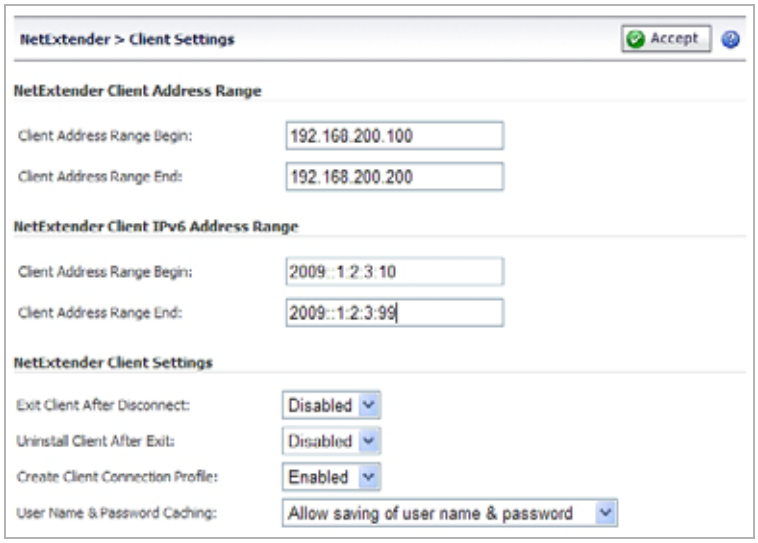
NetExtender > Client Settings

This section provides an overview of the **NetExtender > Client Settings** page and a description of the configuration tasks available on this page.

NetExtender > Client Settings Overview

The **NetExtender > Client Settings** page allows the administrator to specify the client address range.

Figure 24 NetExtender > Client Settings



Configuring the Global NetExtender IP Address Range

The **NetExtender > Client Settings** page allows the administrator to specify the global client address range. The address range can be specified for both IPv4 and, on SonicWALL SSL-VPN models 2000 and higher, IPv6. An IPv6 address pool for NetExtender is optional, while an IPv4 address pool is required. The global NetExtender IP range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as 192.168.200.100 to 192.168.200.115).

The range should fall within the same subnet as the interface to which the SSL-VPN appliance is connected, and in cases where there are other hosts on the same segment as the SSL-VPN appliance, it must not overlap or collide with any assigned addresses. You can determine the correct subnet in one of the following ways:

- You may leave the NetExtender range at the default (192.168.200.100 to 192.168.200.200).

- Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 192.168.50.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 192.168.50.220 to 192.168.50.250, providing they are not already in use.
- Select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.250, providing they are not already in use.

To specify your global NetExtender address range, perform the following steps:

Step 1 Navigate to the **NetExtender** > **Client Settings** page.

Step 2 Under **NetExtender Client Address Range**, supply a beginning client IPv4 address in the **Client Address Range Begin** field.

Step 3 Supply an ending client IPv4 address in the **Client Address Range End** field.

Step 4 On SonicWALL SSL-VPN models 2000 and higher, under **NetExtender Client IPv6 Address Range**, optionally supply a beginning client IPv6 address in the **Client Address Range Begin** field.

Step 5 If using IPv6, supply an ending client IPv6 address in the **Client Address Range End** field.

Step 6 Click **Accept**.

Step 7 The **Status** message displays **Update Successful. Restart for current clients to obtain new addresses.**

Configuring Global NetExtender Settings

SonicWALL SSL VPN provides several settings to customize the behavior of NetExtender when users connect and disconnect. To configure global NetExtender client settings, perform the following steps:

Step 1 Navigate to the **NetExtender** > **Client Settings** page.

Step 2 The following options can be enabled or disabled for all users:

- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users will have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users will have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL VPN Server name, the Domain name and optionally the username and password.

Step 3 The **User Name & Password Caching** options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are **Allow saving of user name only**, **Allow saving of user name & password**, and **Prohibit saving of user name & password**. These options enable administrators to balance security needs against ease of use for users.

Step 4 Click **Accept**.

NetExtender > Client Routes

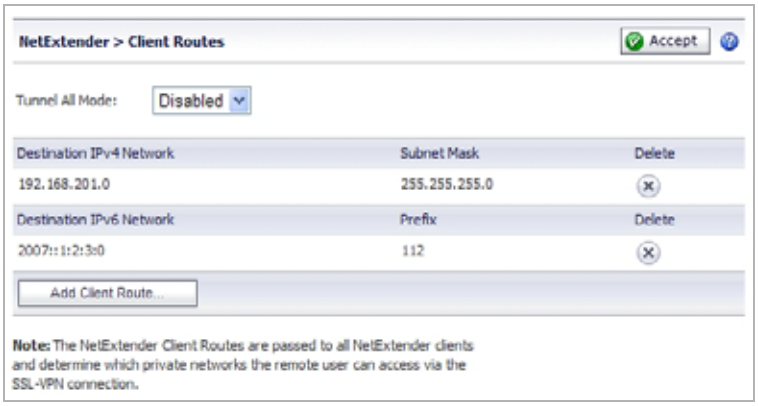
This section provides an overview of the **NetExtender > Client Routes** page and a description of the configuration tasks available on this page.

NetExtender > Client Routes Overview

The **NetExtender > Client Routes** page allows the administrator to add and configure client routes.

Note IPv6 client routes are supported only on SonicWALL SSL-VPN models 2000 and higher.

Figure 25 NetExtender > Client Routes



Adding NetExtender Client Routes

The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote user can access via the SSL VPN connection.

Note With group access policies, all traffic is allowed by default. This is the opposite of the default behavior of SonicWALL Unified Threat Management (UTM) appliances, where all inbound traffic is denied by default. If you do not create policies for your SSL-VPN appliance, then all NetExtender users may be able to access all resources on your internal network(s).

Additional allow and deny policies may be created by destination address or address range and by service type.

Note The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.

User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address.

To add NetExtender client routes, perform the following steps:

Step 1 Navigate to the **NetExtender** > **Client Routes** page.

Step 2 Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for this user—including traffic destined to the remote users' local network—over the SSL VPN NetExtender tunnel.

Step 3 Click the **Add Client Route** button. The **Add Client Route** dialog box displays.

Step 4 In the **Add Client Route** dialog box, in the **Destination Network** field, type the IP address of the trusted network to which you would like to provide access with NetExtender. For example, if you are connecting to an existing DMZ with the network 192.168.50.0/24 and you want to provide access to your LAN network 192.168.168.0/24, you would enter 192.168.168.0.

On SonicWALL SSL-VPN models 2000 and higher, you can enter an IPv6 route in the **Destination Network** field, in the form 2007::1:2:3:0.

Step 5 For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

Step 6 Click **Add**.

Step 7 Repeat this procedure for all necessary routes.

NetExtender User and Group Settings

Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it. This section contains the following subsections:

- "Configuring User-Level NetExtender Settings" section on page 164
- "Configuring Group-Level NetExtender Settings" section on page 167

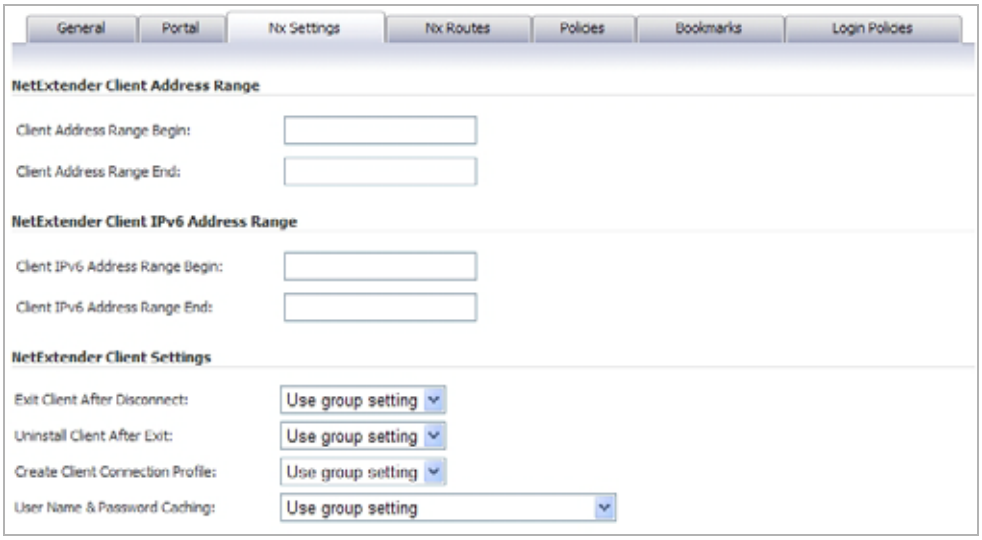
Configuring User-Level NetExtender Settings

All of the global settings for NetExtender (IP address ranges, client routes, and client connection settings) can be configured at the user and group levels. Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it. To configure custom settings for individual users, perform the following steps:

Step 1 Navigate to the **Users > Local Users** page.

Step 2 Click on the configure icon  for the user you want to edit. The **Edit User** window is launched.

Step 3 Click on the **Nx Settings** tab.



Configuring User Client IP Address Range

Step 1 To configure an IPv4 address range for this user, enter the beginning of the range in the **Client Address Range Begin** field and the end of the range in the **Client Address Range End** field.

Step 2 To give this user the same IP address every time the user connects, enter the IP address in both fields.

Step 3 On SonicWALL SSL-VPN models 2000 and higher, to configure an IPv6 address range for this user, enter the beginning of the range in the **Client IPv6 Address Range Begin** field and the end of the range in the **Client IPv6 Address Range End** field. IPv6 configuration is optional.

Step 4 To give this user the same IPv6 address every time the user connects, enter the IP address in both fields.

Tip Unless more than one user will be using the same username, which is not recommended, there is no need to configure more than one IP address for the user client IP address range.

Step 5 Click **OK**.

Configuring User NetExtender Settings

The following NetExtender settings can be configured for the user:

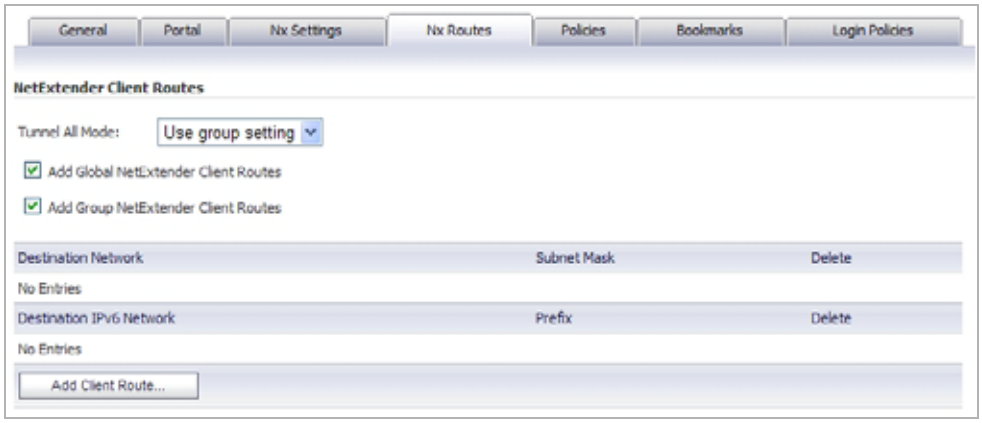
- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SSL VPN server. To reconnect, users will have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users will have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL VPN Server name, the Domain name and optionally the username and password.

- The **User Name & Password Caching** options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are **Allow saving of user name only**, **Allow saving of user name & password**, and **Prohibit saving of user name & password**. These options enable administrators to balance security needs against ease of use for users.

To have the user inherit the NetExtender settings from the group it belongs to (or from the global NetExtender settings if the user does not belong to a group), select **Use Group Settings** for any of the above options.

Configuring User NetExtender Routes

Step 1 To add a NetExtender client route that will only be added to this user, click the **Nx Routes** tab in the **Edit User Settings** window.



Step 2 **Add Client Route** button.

Step 3 Type the IPv4 or, on SonicWALL SSL-VPN models 2000 and higher, IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.

Step 4 For an IPv4 client route, type the subnet mask in the **Subnet Mask/Prefix** field. For an IPv6 client route, type the prefix in this field.

Step 5 Click **Add**.

Step 6 Repeat steps 1 through 5 for all necessary routes.

Step 7 Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for this user—including traffic destined to the remote users' local network—over the SSL VPN NetExtender tunnel.

Step 8 To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to the user, select the **Add Global NetExtender Client Routes** checkbox.

Step 9 To also add the group NetExtender client routes for the group the user belongs to, select the **Add Group NetExtender Client Routes** checkbox. Group NetExtender routes are configured on the **NetExtender** tab of the **Edit Group** window, which is accessed through the **Users > Local Groups** page.

Step 10 Click **OK**.

Note When using an external authentication server, local usernames are not typically configured on the SonicWALL SSL-VPN appliance. In such cases, when a user is successfully authenticated, a local user account is created with the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** settings enabled.

Configuring Group-Level NetExtender Settings

Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need of configuring firewall rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it. To configure custom settings for groups, perform the following steps:

Step 1 Navigate to the **Users > Local Groups** page.

Step 2 Click on the configure icon for the group you want to edit. The **Edit Group Settings** window is launched.

Step 3 Click on the **Nx Settings** tab.

Configuring Group Client IP Address Range

Step 1 To configure an IPv4 address range for this group, enter the beginning of the range in the **Client Address Range Begin** field and the end of the range in the **Client Address Range End** field.

Step 2 On SonicWALL SSL-VPN models 2000 and higher, to configure an IPv6 address range for this group, enter the beginning of the range in the **Client IPv6 Address Range Begin** field and the end of the range in the **Client IPv6 Address Range End** field. IPv6 configuration is optional.

Step 3 Click **OK**.

Configuring Group NetExtender Settings

The following NetExtender settings can be configured for the user:

- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SSL VPN server. To reconnect, users will have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users will have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL VPN Server name, the Domain name and optionally the username and password.
- The **User Name & Password Caching** options provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are **Allow saving of user name only**, **Allow saving of user name & password**, and **Prohibit saving of user name & password**. These options enable administrators to balance security needs against ease of use for users.

To have the user inherent the NetExtender settings from the global NetExtender settings, select **Use Global Settings** for any of the above options.

Configuring Group NetExtender Routes

Step 1 To add a NetExtender client route that will only be added to this user, click the **Nx Routes** tab in the **Edit User Settings** window.

Step 2 To add a NetExtender client route that will only be added to users in this group, click the **Add Client Route** button.

Step 3 Type the IPv4 or, on SonicWALL SSL-VPN models 2000 and higher, IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.

Step 4 For an IPv4 route, type the subnet mask in the **Subnet Mask/Prefix** field. For an IPv6 route, type the prefix in the **Subnet Mask/Prefix** field.

Step 5 Click **Add**.

Step 6 Repeat this procedure for all necessary routes.

Step 7 Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for this user—including traffic destined to the remote users' local network—over the SSL VPN NetExtender tunnel.

Step 8 To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to users in this group, select the **Add Global NetExtender Client Routes** checkbox.

Step 9 Click **OK**.

Chapter 7: Virtual Assist Configuration

This chapter provides information and configuration tasks specific to the **Virtual Assist** pages on the SonicWALL SSL VPN Web-based management interface.

Supported on SonicWALL SSL-VPN models 2000 and higher, Virtual Assist is an easy to use tool that allows SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Providing support to customers is traditionally a costly and time consuming aspect of business. Virtual Assist creates a simple to deploy, easy to use remote support solution.

For more information on Virtual Assist concepts, see the "Virtual Assist Overview" section on page 31.

This chapter contains the following sections:

Virtual Assist > Status

This section provides an overview of the **Virtual Assist > Status** page and a description of the configuration tasks available on this page.

Virtual Assist > Status

The **Virtual Assist > Status** page displays a summary of current active requests, including the customer name, the summary of their issue they provided, the status of the Virtual Assist session, and which technician is assisting the customer.

On the right side of the screen, **Streaming Updates** indicates that changes to the status of customers will be dynamically updated. Click **ON/OFF** to enable/disable Streaming Updates, respectively.

Click the **Logout** button to remove a customer from the queue. If the customer is currently in a session, both the customer and technician are disconnected.

For information about using Virtual Assist as a technician, see the following sections:

- “Launching a Virtual Assist Technician Session” section on page 33
- “Performing Virtual Assist Technician Tasks” section on page 36

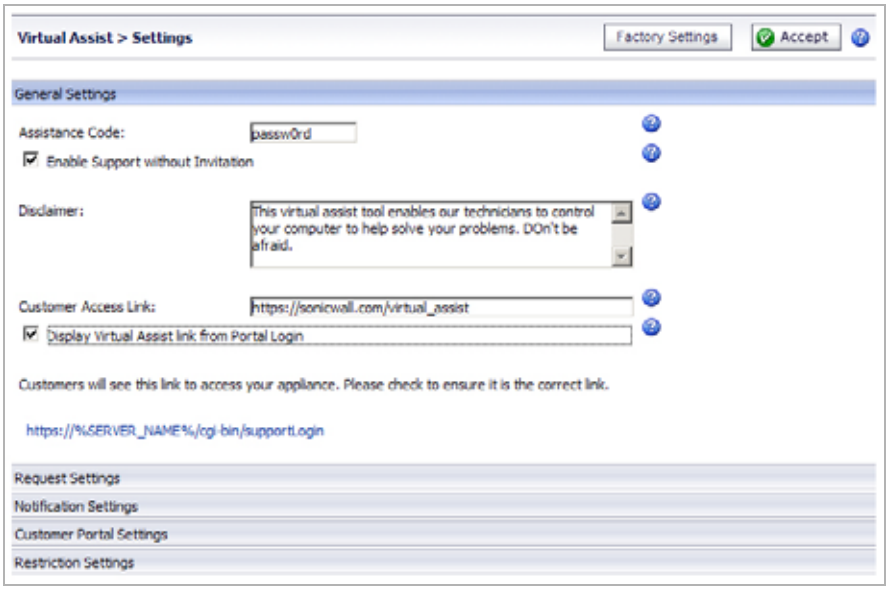
Virtual Assist > Settings

This section describes the **Virtual Assist > Settings** page and the configuration tasks available on this page. The Virtual Assist options are divided into the following tabs:

General Settings

To configure Virtual Assist general settings, perform the following tasks:

Step 1 Navigate to the **Virtual Assist > Settings** page.



Step 2 To require customers to enter a password before being allowed to access Virtual Assist, enter the password in the **Assistance Code** window.

Step 3 (Optional) Select **Enable Support without Invitation** to allow customers who have not received an email invitation to request assistance. If this is disabled, customers can receive assistance only if they are explicitly invited by a technician.

Step 4 (Optional) To present customers with a legal disclaimer, instructions, or any other additional information, enter the text in the **Disclaimer** field. HTML code is allowed in this field. Customers will be presented with the disclaimer and required to click "Accept" before beginning a Virtual Assist session.

Step 5 (Optional) To change the URL that customers use to access Virtual Assist, enter it in the **Customer Access Link** field. This may be necessary if your SonicWALL SSL-VPN appliance requires a different access URL when outside the network.

The default URL is **https://***server-name***cgi-bin/supportLogin**. When entering a URL, the **https://** will be automatically prepended to your entry, and **/cgi-bin/supportLogin** will be automatically appended.

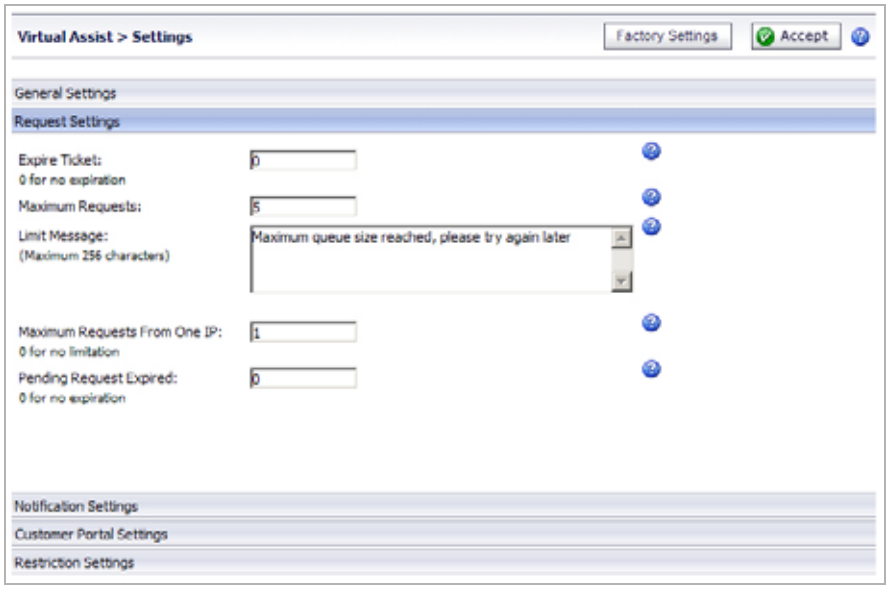
For example, if you enter **test.com/virtual_assist** in the **Customer Access Link** field, the URL will be **https://test.com/virtual_assist/cgi-bin/supportLogin**.

Step 6 To include a link to Virtual Assist on the portal login page, select the **Display Virtual Assist link from Portal Login** checkbox. Customers can then click on a link to go directly to the Virtual Assist portal login page without having to login to the Virtual Office.

Request Settings

To configure Virtual Assist request settings, perform the following tasks:

Step 1 On the **Virtual Assist > Settings** page, click the **Request Settings** tab at the bottom of the page.



Step 2 To have Virtual Assist requests timeout after a certain amount of time, enter a value in the **Expire Ticket** field. The default is **0**, which means there is no expiration. After the timeout duration has passed, customers will have to reinitiate their Virtual Assist request.

Step 3 To limit the number of customers allowed in the Virtual Assist queue, enter a value in the **Maximum Request** field.

Step 4 Optionally you can customize the message that is displayed to customers when the queue is full in the **Limit Message** field. The message is limited to 256 characters.

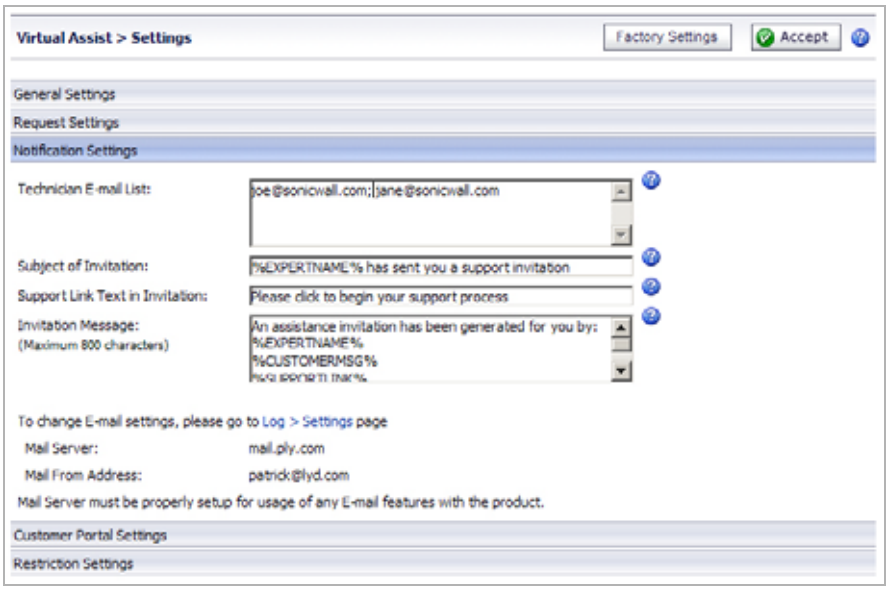
Step 5 Entering a value in the **Maximum requests From One IP** field can be useful if individual customers are repeatedly requesting help. However, this may cause problems for customers using DHCP behind a single IP address. The default **0** does not limit request from individual IP addresses.

Step 6 Enter a value in the **Pending Request Expired** field to have customers automatically removed from the queue if they are not assisted within the specified number of minutes. The default **0** does not remove unassisted customers.

Notification Settings

To configure Virtual Assist notification settings, perform the following tasks:

Step 1 On the **Virtual Assist > Settings** page, click the **Notification Settings** tab at the bottom of the page.



Step 2 To automatically email support technicians when a customer logs in to the Virtual Assist queue, enter the technicians' emails in the **Technician Email List**. Separate multiple emails with semi-colons (the ; symbol).

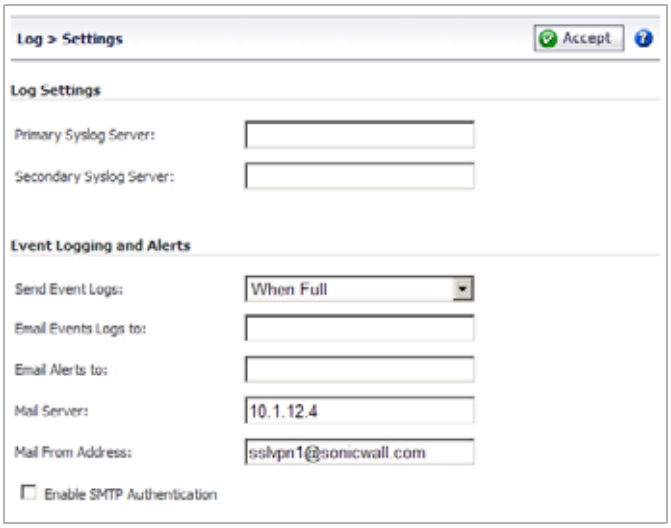
Step 3 The next three fields allow you to customize the email invitation:

- **Subject of Invitation** - The email subject line.
- **Support Link Text in Invitation** - Text that introduces the link to the URL for accessing Virtual Assist.
- **Invitation Message** - The body of the invitation email message.

These three fields support the following variables to customize and personalize the invitation:

- %EXPERTNAME% - The name of the technician sending the invitation email.
- %CUSTOMERMSG% - The disclaimer configured on the **General Settings** tab.
- %SUPPORTLINK% - The URL for accessing Virtual Assist.
- %ACCESSLINK% - The URL for accessing the SSL VPN Virtual Office.

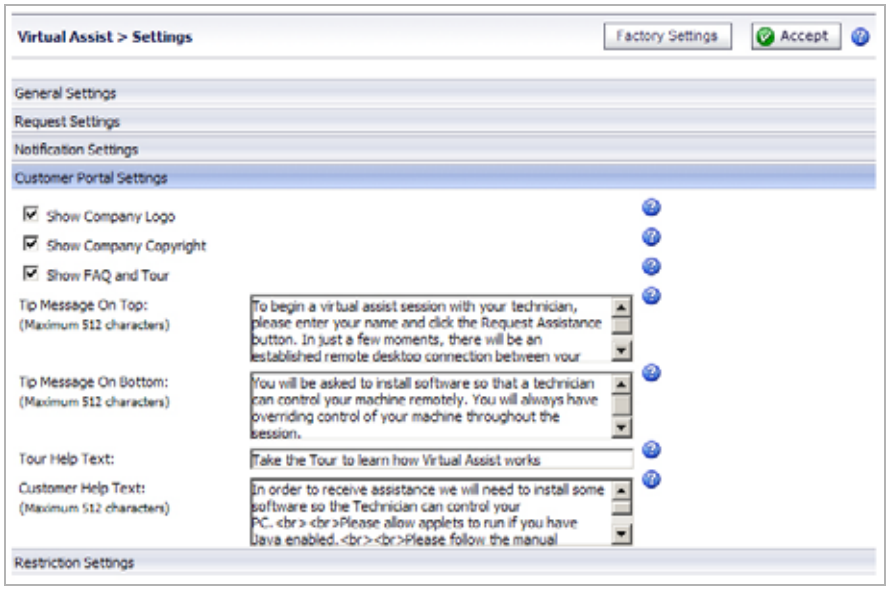
Note The currently configured mail server and email return address are listed at the bottom of the **Virtual Assist > Settings** page. To enable technicians to receive notification emails and to email Virtual Assist invitations to customers, a mail server must be configured on the **Log > Settings** page. An accurate technician email address will also allow blocked email notification to the technician in deployments where a third-party email filter may block emails sent to the customer without providing an error to the Virtual Assist client.



Customer Portal Settings

To customize the appearance of the Virtual Assist customer portal, perform the following tasks:

Step 1 On the **Virtual Assist > Settings** page, click the **Customer Portal Settings** tab at the bottom of the page.



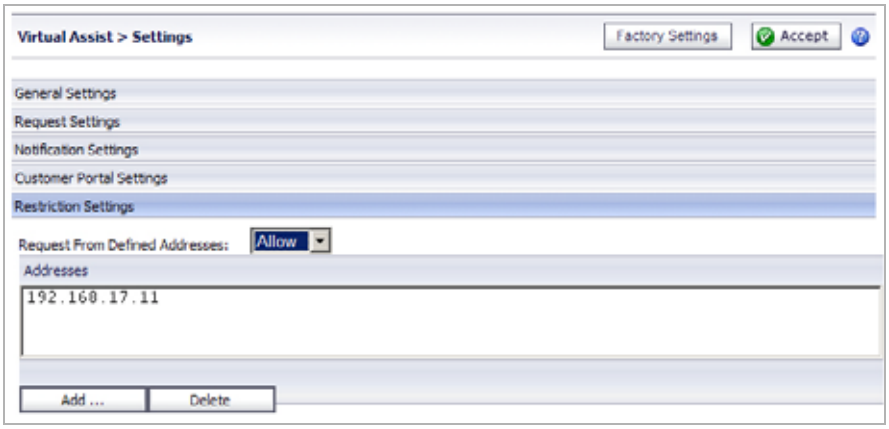
Step 2 Configure the following options to customize the appearance of the customer portal

- **Show Company Logo** - Displays the company logo that is configured on the **Logo** tab of the **Edit Portal** window.
- **Show Company Copyright** - Displays the copyright at the bottom of the page.
- **Show FAQ and Tour** - Displays links to the Virtual Assist FAQ and tour on the customer request page.
- **Tip Message On Top** - Customizes the text that is displayed above the Virtual Assist link.
- **Tip Message On Bottom** - Customizes the text that is displayed below the Virtual Assist link.
- **Tour Help Text** - Customizes the text that is displayed above the link for the Virtual Assist tour.
- **Customer Help Text** - Customizes the text that is displayed after the customer clicks the Virtual Assist link.

Restriction Settings

To configure Virtual Assist restriction settings, perform the following tasks:

Step 1 On the **Virtual Assist > Settings** page, click the **Restriction Settings** tab at the bottom of the page.



Step 2 To deny Virtual Assist requests from specific IP addresses or networks, select **Deny** from the **Request From Defined Addresses** pull-down menu.

Step 3 To allow Virtual Assist requests only from specific IP addresses or networks, select **Allow** from the **Request From Defined Addresses** pull-down menu.

Step 4 To add an IP address or network to the Deny or Allow list, click the **Add...** button. The **Admin Addresses** window displays.

Step 5 In the **Source Address Type** pull-down menu, select which of the following you want to specify:

- IP Address
- IP Network
- IPv6 Address
- IPv6 Network

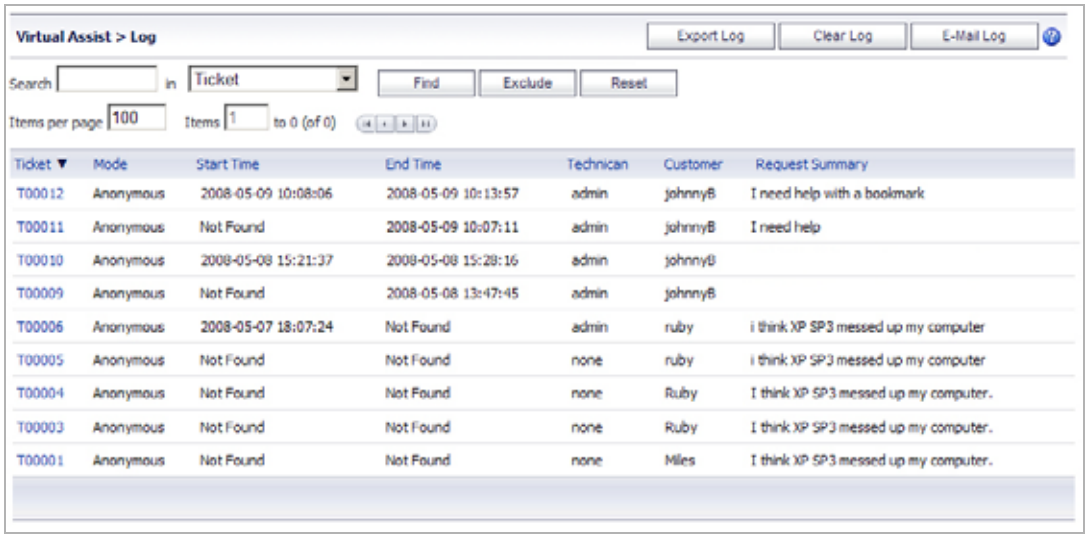
Step 6 Enter the information to define the address or network and click **Add**.

Step 7 To delete a configured restriction setting, select the desired address in the **Addresses** field and click Delete. The address will be removed from the field.

Virtual Assist > Log

The **Virtual Assist > Log** page provides access to detailed information about previous Virtual Assist sessions. The **Log** page displays a summary of recent sessions.

The Technician's activities while servicing the customer are now fully logged, including the Technician ID, the time of service, information about the customer's and Technician's computers, the chat dialog, the customer request login, if the customer exit prior to servicing, and Technician input after the end of the session.



Ticket ▼	Mode	Start Time	End Time	Technican	Customer	Request Summary
T00012	Anonymous	2008-05-09 10:08:06	2008-05-09 10:13:57	admin	johnnyB	I need help with a bookmark
T00011	Anonymous	Not Found	2008-05-09 10:07:11	admin	johnnyB	I need help
T00010	Anonymous	2008-05-08 15:21:37	2008-05-08 15:28:16	admin	johnnyB	
T00009	Anonymous	Not Found	2008-05-08 13:47:45	admin	johnnyB	
T00006	Anonymous	2008-05-07 18:07:24	Not Found	admin	ruby	i think XP SP3 messed up my computer
T00005	Anonymous	Not Found	Not Found	none	ruby	i think XP SP3 messed up my computer
T00004	Anonymous	Not Found	Not Found	none	Ruby	I think XP SP3 messed up my computer.
T00003	Anonymous	Not Found	Not Found	none	Ruby	I think XP SP3 messed up my computer.
T00001	Anonymous	Not Found	Not Found	none	Miles	I think XP SP3 messed up my computer.

Click on the **Ticket Number** to view details about a session, or ticket. The **Virtual Assist > Log > <ticket number>** page is displayed. Click **Save Log** to save the information on the page. To return to the **Virtual Assist > Log** summary page, click **Back**.

Click **Export Log** to save a zip file containing the full text of all logged sessions. The log contains a summary file and a detail file for each session. The files can be viewed in Microsoft Word.

Click **Clear Log** to erase all log messages.

Click **Email Log** to send the log to the email address configured on the **Log > Settings** page.

The **Search** options allow you to filter the log messages. Note that the search is case sensitive. In the pull-down menu, select the field you want to search in. Click **Search** to only display messages that match the search string. Click **Exclude** to hide messages that match the search string. Click **Reset** to display all messages.

Change the value in the **Items** per page field to display more or fewer log messages. Click the forward or backward arrows to scroll through the pages of the log messages.

Click any of the headings to sort the log messages alphabetically by heading.

Virtual Assist > Licensing

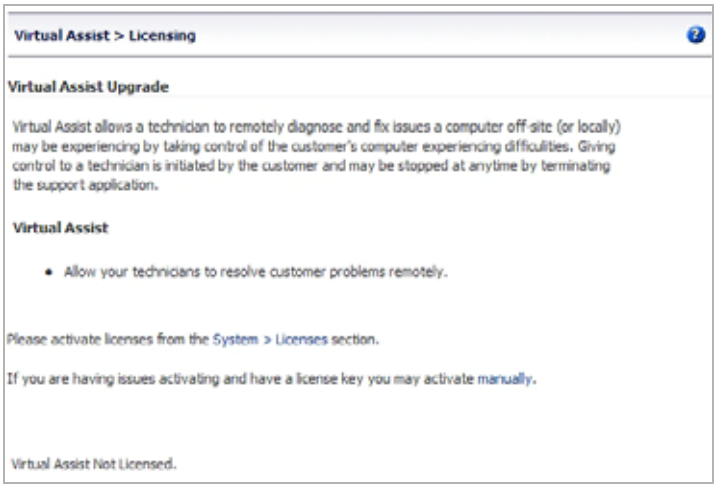
This section provides an overview of the **Virtual Assist > Licensing** page and a description of the configuration tasks available on this page.

Virtual Assist > Licensing Overview

Virtual Assist is a licensed service. The **Virtual Assist > Licensing** page allows the administrator to view the license status for Virtual Assist. You can purchase licenses for one Technician, two Technicians, or more. At the bottom of the **Virtual Assist > Licensing** page, you can see the number of Technicians that are licensed, or if the feature is not licensed.

The page directs the administrator to activate or upgrade the license for this feature on the **System > Licenses** page.

The same content from the **Virtual Assist > Licensing** page is also displayed when you navigate to **Virtual Assist > Status** on a SonicWALL SSL-VPN appliance that does not have a valid Virtual Assist license.



Enabling Virtual Assist

To configure Virtual Assist on your SonicWALL SSL-VPN model 2000 or higher security appliance, perform the following tasks:

Step 1 To purchase and activate a Virtual Assist license, navigate to **System > Licensing** and click on the link to **Activate, Upgrade, or Renew services.**

For more information, see the "System > Licenses" section on page 64.

Step 2 By default, Virtual Assist is disabled on all portals that were created before the Virtual Assist license is purchased. Virtual Assist is enabled by default on portals that are created after Virtual Assist is licensed. To enable Virtual Assist on a portal, go to the **Portals > Portals** page and click the **Configure** icon for the desired portal. To create a new portal, go to the **Portals > Portals** page and click the **Add Portal** button. See the "Portals > Portals" section on page 106.

Step 3 In the **Edit Portal** window that displays, click the **Virtual Assist** tab.

Step 4 Click on the **Enable Virtual Assist for this Portal** checkbox and click **OK**. Virtual Assist is now enabled and ready to use. SSL VPN users will now see the Virtual Assist icon on the Virtual Office page.

Step 5 Optionally, you can customize all of the Virtual Assist settings for this individual portal using the tabs on this window.

Virtual Assist is now enabled and ready to use. SSL VPN users will now see the **Virtual Assist** icon on the Virtual Office page.

Chapter 8: Web Application Firewall Configuration

This chapter provides information and configuration tasks specific to the **Web Application Firewall** pages on the SonicWALL SSL VPN Web-based management interface.

Supported on SonicWALL SSL-VPN models 2000 and higher, Web Application Firewall is subscription-based software that runs on the SonicWALL SSL-VPN appliance and protects Web applications running on servers behind the SSL-VPN. Web Application Firewall also provides real-time protection for resources such as HTTP(S) bookmarks, Citrix bookmarks, offloaded Web applications, and the SSL-VPN management interface and user portal that run on the SonicWALL SSL-VPN appliance itself.

For more information on Web Application Firewall concepts, see the “Web Application Firewall Overview” section on page 43.

This chapter contains the following sections:

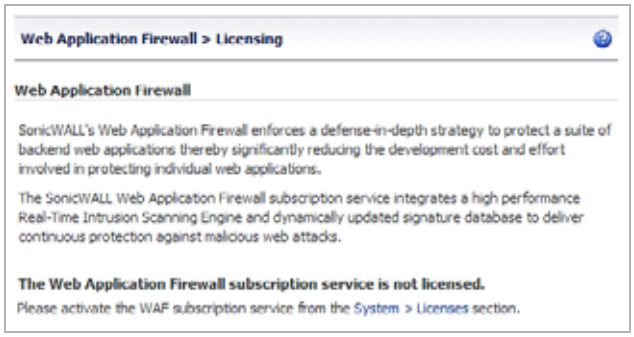
Licensing Web Application Firewall

SonicOS SSL VPN Web Application Firewall must be licensed before you can begin using it. You can access the MySonicWALL Web site directly from the SSL-VPN management interface to obtain a license.

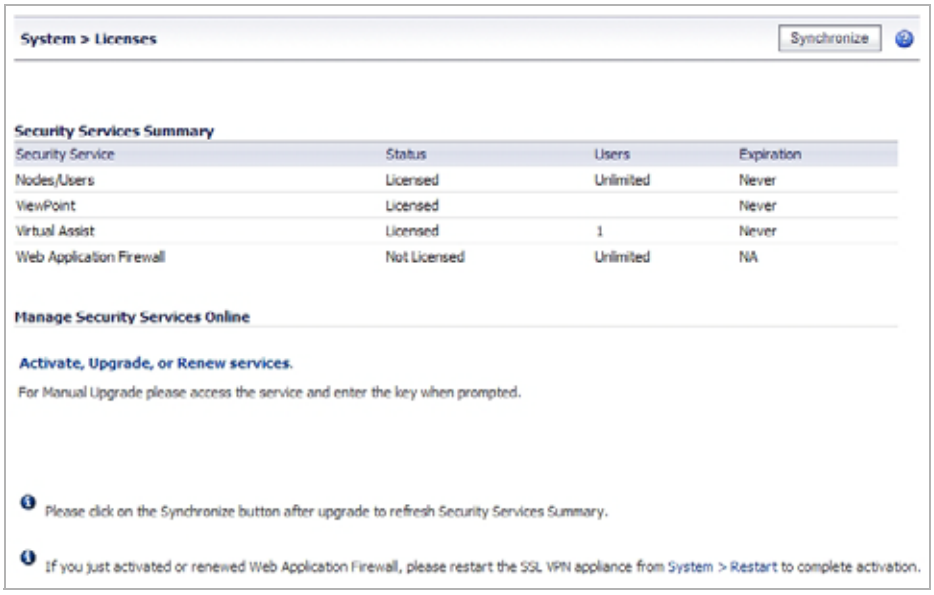
The Web Application Firewall > Licensing page in the SonicOS SSL VPN management interface provides a link to the System > Licenses page, where you can connect to MySonicWALL and purchase the license or start a free trial. You can view all system licenses on the System > Licenses page of the management interface.

To view license details and obtain a license on MySonicWALL for Web Application Firewall, perform the following steps:

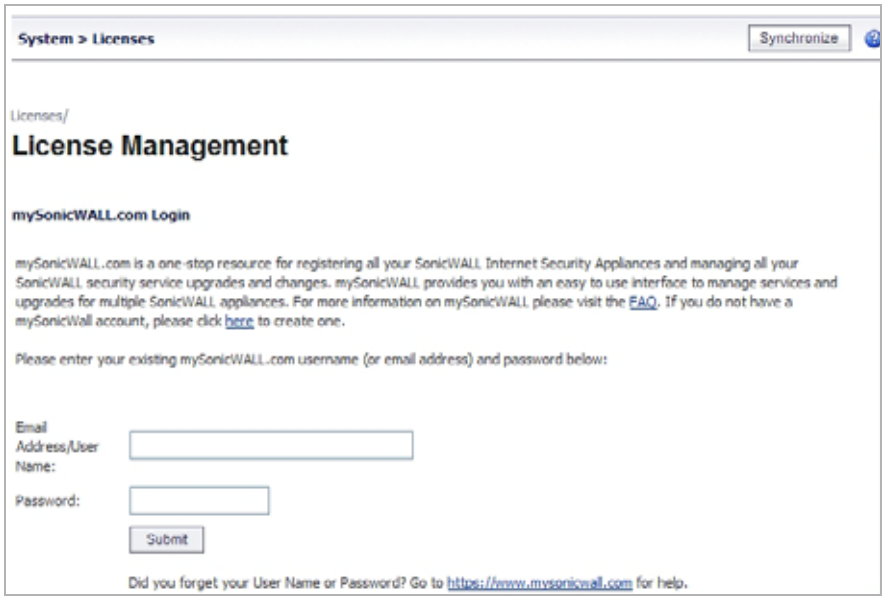
Step 1 Log in to your SonicWALL SSL-VPN appliance and navigate to **Web Application Firewall > Licensing**.



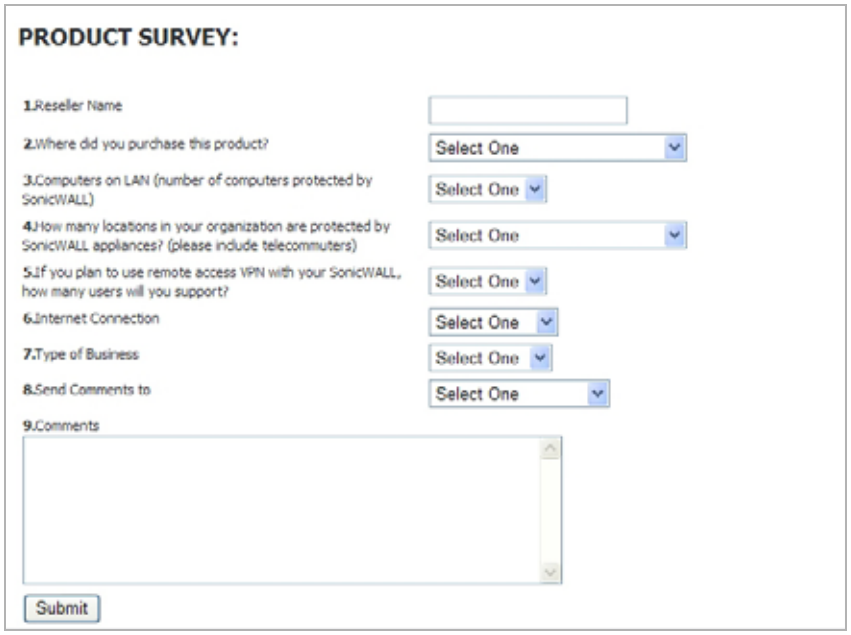
Step 2 If Web Application Firewall is not licensed, click the **System > Licenses** link. The System > Licenses page is displayed.



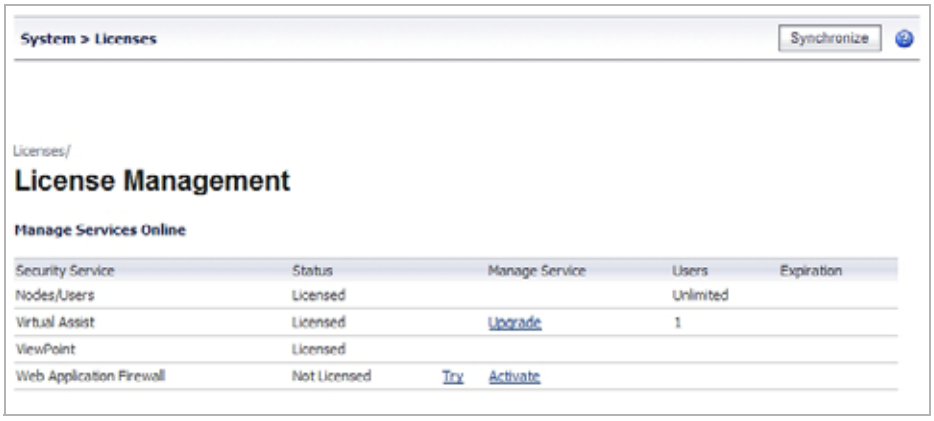
Step 3 Under Manage Security Services Online, click the **Activate, Upgrade, or Renew services** link. The MySonicWALL Login page is displayed.



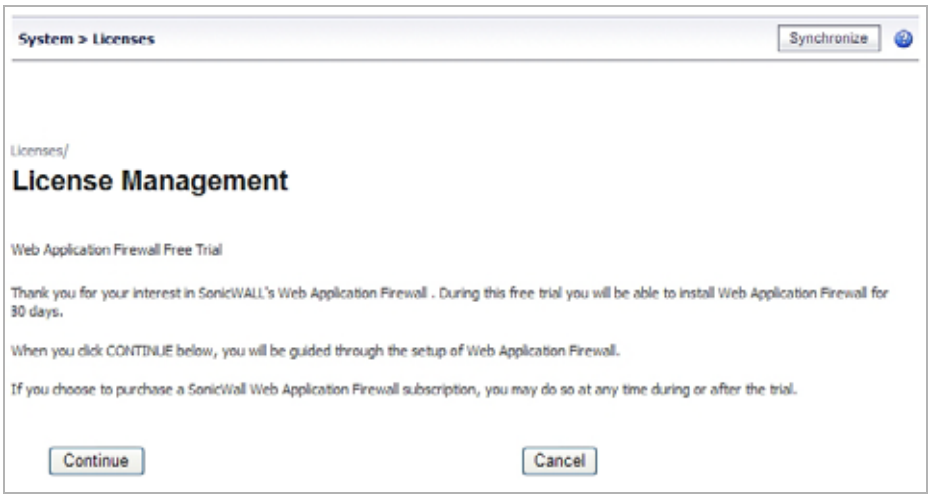
Step 4 Type your MySonicWALL credentials into the fields, and then click **Submit**. The Product Survey page is displayed.



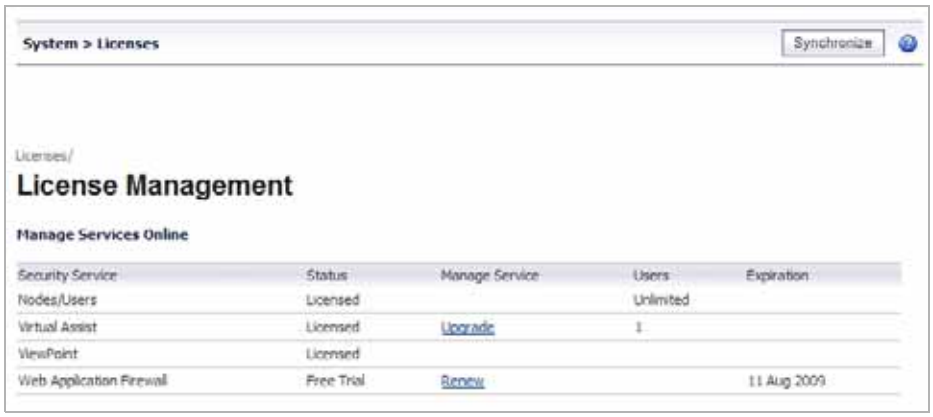
Step 5 Fill out the survey and then click **Submit**. The System > Licenses page is displayed.



Step 6 Click **Try** to start a 30 day free trial, or click **Activate** to subscribe to the service for 1 year. The screen below is displayed after selecting the free trial.



Step 7 Click **Synchronize** to view the license on the System > Licenses page.



Web Application Firewall is now licensed on your SonicWALL SSL-VPNappliance. Navigate to Web Application Firewall > Settings to enable it, and then restart your appliance to completely activate Web Application Firewall.

Configuring Web Application Firewall

Note Web Application Firewall requires the purchase of an additional license.

To configure the Web Application Firewall feature, see the following sections:

Viewing and Updating Web Application Firewall Status

The Web Application Firewall > Status page provides status information about the Web Application Firewall service and signature database, and lists the threats that have been detected and/or prevented. The Synchronize button allows you to download the latest signatures from the SonicWALL online database. You can view details about the threats, or clear the threat list. The Severity column of the threat list is color coded for quick reference, as follows:

- High severity threats – Red
- Medium severity threats – Orange
- Low severity threats – Black

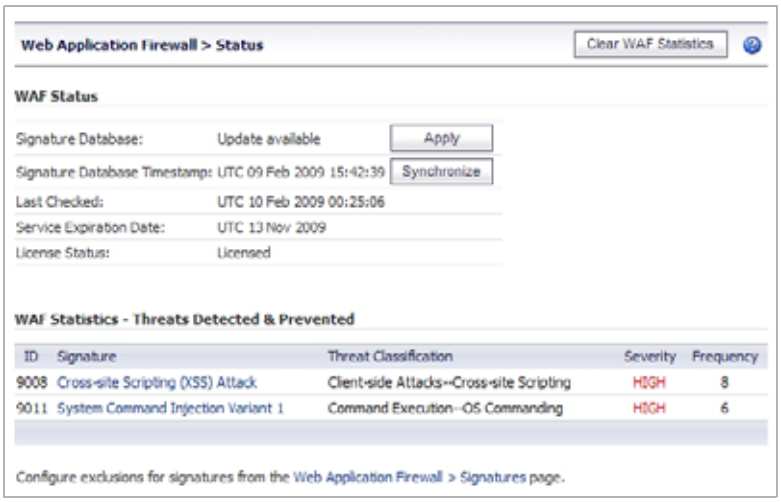
See the following sections:

Signature and License Status

To view the status of the signature database and Web Application Firewall service license, and synchronize the signature database, perform the following steps in the appliance management interface:

Step 1 Navigate to **Web Application Firewall > Status**. The WAF Status section displays the following information:

- Status of updates to the signature database
- Timestamp of the signature database
- Time that the system last checked for available updates to the signature database
- Expiration date of the Web Application Firewall subscription service
- Status of the Web Application Firewall license



Step 2 If updates are available for the signature database, the **Apply** button is displayed. Click **Apply** to download the updates.

You can update and apply new signatures automatically on the Web Application Firewall > Settings page. If this automatic update option is enabled, the **Apply** button disappears from the Web Application Firewall > Status screen as soon as the new signatures are automatically applied.

Step 3 To synchronize the signature database with the SonicWALL online database server, click **Synchronize**. The timestamp is updated.

Threat Statistics

The Status page displays statistics on all threats detected since Web Application Firewall was activated.

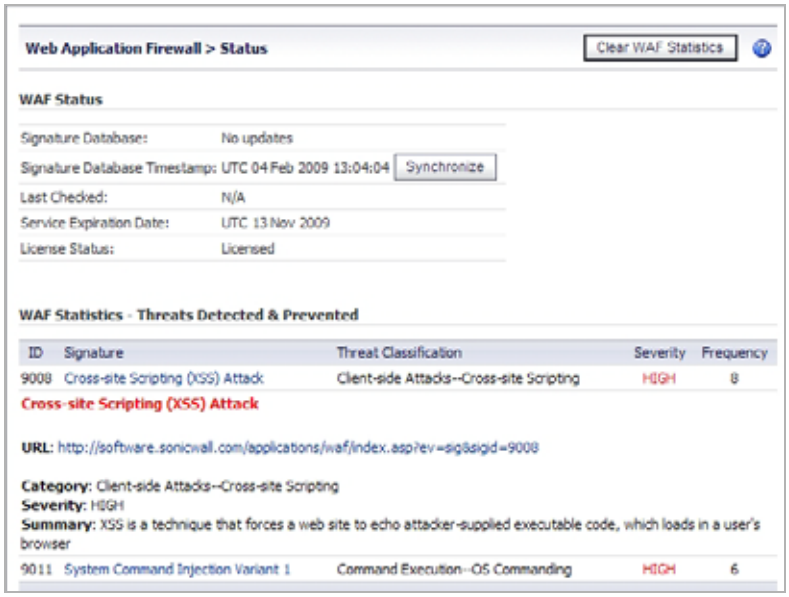
To view and hide threat details, and clear the threat list, perform the following steps:

Step 1 Navigate to **Web Application Firewall > Status**. The list of detected or prevented threats is displayed in the **WAF Statistics - Threats Detected & Prevented** table.

Step 2 To display details about a threat, click on the threat. The details include the following:

- URL – The URL to the SonicWALL knowledge base for this threat

- Category – The category of the threat
- Severity – The severity of the threat, either high, medium, or low
- Summary – A short description of how the threat behaves

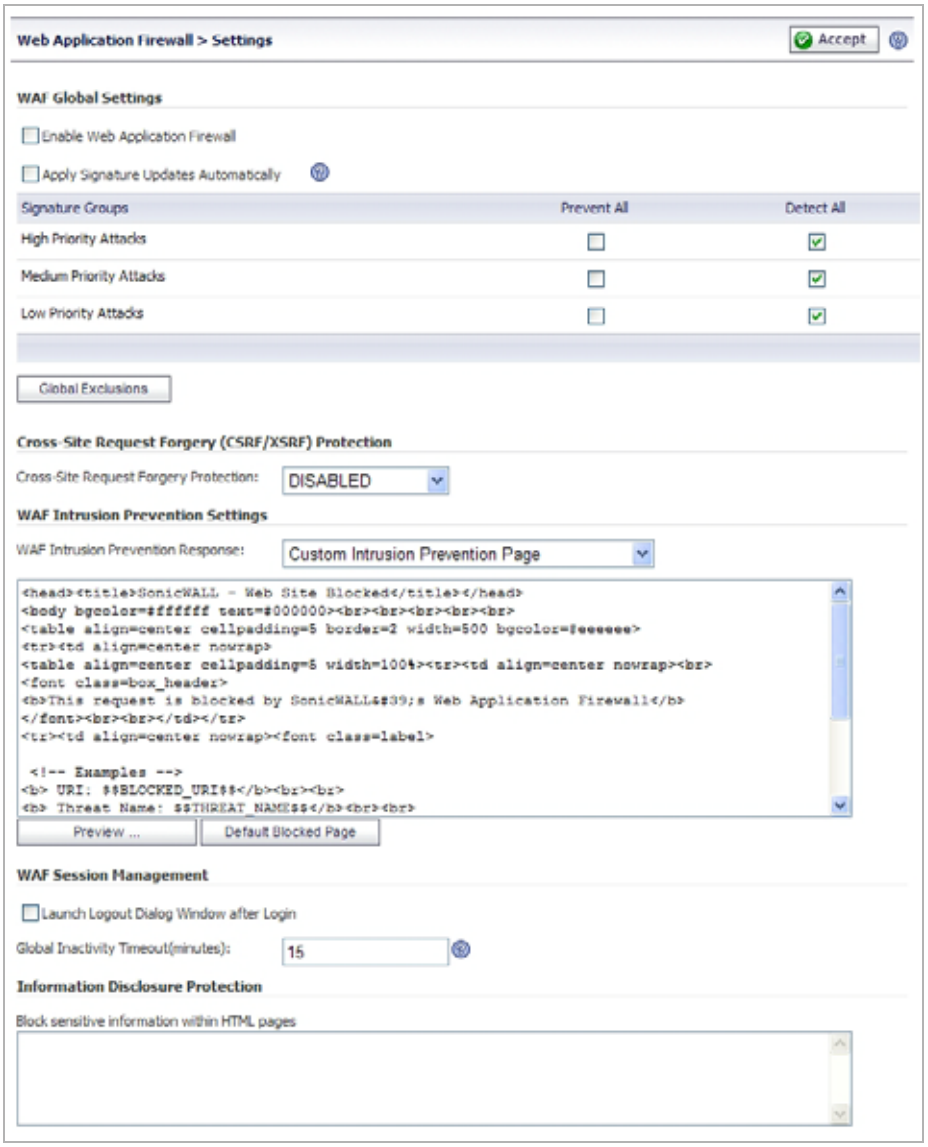


Step 3 To collapse the threat details, click the threat link again.

Step 4 To clear the threat list, click the **Clear WAF Statistics** button on the top right corner of the page.

Configuring Web Application Firewall Settings

The Web Application Firewall > Settings page allows you to enable and disable Web Application Firewall on your SonicWALL SSL-VPN appliance globally and by attack priority. You can individually specify detection or prevention for three attack classes: high, medium, and low priority attacks. This page also provides configuration options for globally excluding certain hosts from inspection by Web Application Firewall.



The following sections describe the procedures for enabling and configuring Web Application Firewall globally and by attack priority:

- “Enabling Web Application Firewall and Configuring Settings” on page 187
- “Configuring Global Exclusions” on page 189

Enabling Web Application Firewall and Configuring Settings

To enable and activate Web Application Firewall, you must select the checkbox to globally enable it and select at least one of the checkboxes in the Signature Groups table. The settings on this page allow you to globally manage your network protection against attacks by selecting the level of protection for high, medium, or low priority attacks. You can also clear the global **Enable Web Application Firewall** checkbox to temporarily disable Web Application Firewall without losing any of your custom configuration settings.

You can enable automatic signature updates on this page, so that new signatures are automatically downloaded and applied when available. A log entry is generated for each automatic signature update. If a signature is deleted during automatic updating, its associated Exclusion List is also removed. A log entry is generated to record the removal. You can view the log entries on the Web Application Firewall > Log page.

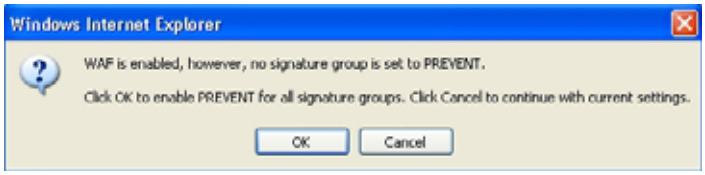
Cross-Site Request Forgery protection settings are also available on this page. When a CSRF attack is detected, log entries are created in both the WAF > Logs and Logs > View pages. For more information about CSRF/XSRF attacks, see “How is Cross-Site Request Forgery Prevented?” on page 47.

To configure global settings for Web Application Firewall, perform the following steps:

Step 1 Log in to your SonicWALL SSL-VPN appliance and navigate to **Web Application Firewall > Settings**.

Step 2 Select the **Enable Web Application Firewall** checkbox.

Step 3 A warning dialog box is displayed if none of the signature groups have **Prevent All** already selected. Click **OK** in the dialog box to set all signature groups to **Prevent All**, or click **Cancel** to leave the settings as they are or to manually continue the configuration.



Step 4 Select the **Apply Signature Updates Automatically** checkbox to enable new signatures to be automatically downloaded and applied when available. You do not have to click the **Apply** button on the Web Application Firewall > Status page to apply the new signatures.

Step 5 Select the desired level of protection for **High Priority Attacks** in the Signature Groups table. Select one of the following options:

- Select the **Prevent All** checkbox to block access to a resource when an attack is detected. Selecting **Prevent All** automatically selects **Detect All**, turning on logging.
- Clear the **Prevent All** checkbox and select the **Detect All** checkbox to log attacks while allowing access to the resource.
- To globally disable all logging and prevention for this attack priority level, clear both checkboxes.

Step 6 Select the desired level of protection for **Medium Priority Attacks** in the Signature Groups table.

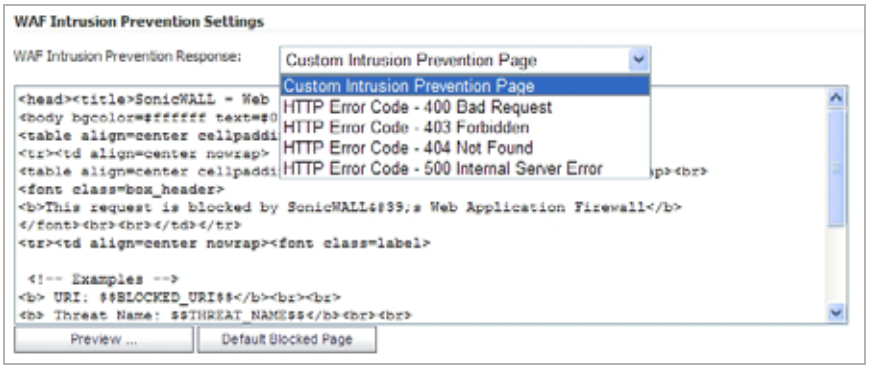
Step 7 Select the desired level of protection for **Low Priority Attacks** in the Signature Groups table.

Step 8 To configure exclusions, refer to the procedures described in the following sections:

- “Configuring Global Exclusions” on page 189
- “Configuring Signature Based Custom Handling and Exclusions” on page 191

Step 9 Select the desired level of protection against CSRF attacks from the Cross-Site Request Forgery Protection drop-down list. You can select **Detect Only** to log these attacks, or **Prevent** to log and block them. Select **Disabled** to disable CSRF protection.

Step 10 Under **WAF Intrusion Prevention Settings**, use the **WAF Intrusion Prevention Response** drop-down list to select the type of error to be displayed when blocking an intrusion attempt.



- To create a custom page, modify the sample HTML in the text box.
- To view the resulting page, click the **Preview** button.
- To reset the current customized error page to the default SonicWALL error page, click the **Default Blocked Page** button and then click **OK** in the confirmation dialog box.

Step 11 Under **WAF Session Management**, select the **Launch Logout Dialog Window after Login** checkbox to display the session logout popup dialog box when the user portal is launched or when a user logs into an application offloaded portal. This feature is enabled by default when Web Application Firewall is licensed.

Step 12 In the **Global Inactivity Timeout** field, type the number of inactive minutes allowed before the user is logged out.

Note To mitigate CSRF attacks, it is important to keep a low idle timeout value for user sessions, such as 10 minutes.

Step 13 Under **Information Disclosure Protection**, type confidential text strings that should not be revealed on any Web site protected by Web Application Firewall into the text box. This text is case insensitive, can include any number of spaces between the words, and cannot include wildcard characters. Add new phrases on separate lines. Each line is pattern matched within any HTML response.

Step 14 Click **Accept**. A dialog box indicates that the SSL-VPN appliance must be restarted to apply the settings. Click **OK** to restart the services or click **Cancel** to leave the previous settings in place.

Configuring Global Exclusions

There are two ways that you can exclude certain hosts from currently configured global Web Application Firewall settings. You can completely disable Web Application Firewall for certain hosts, or you can lower the action level from Prevent to Detect for certain hosts.

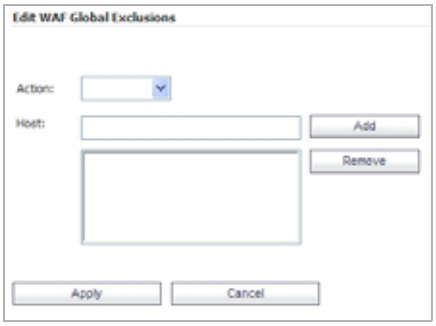
The affected hosts must match the host names used in your HTTP(S) bookmarks and Citrix bookmarks, and the Virtual Host Domain Name configured for an offloaded Web application.

To configure global exclusions, perform the following steps:

Step 1 On the Web Application Firewall > Settings page, click the **Global Exclusions** button.

Step 2 In the Edit Global Exclusions page, select one of the following from the **Actions** drop-down list:

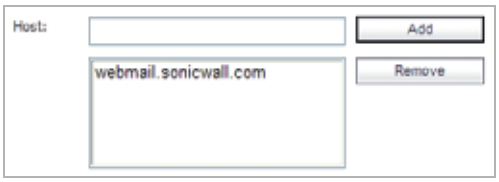
- **Disable** – Disables Web Application Firewall inspection for the host
- **Detect** – Lowers the action level from prevention to detection and logging only for the host



Step 3 In the **Host** field, type in the host entry as it appears in the bookmark or offloaded application. This can be a host name or an IP address. To determine the correct host entry for this exclusion, see “Determining the Host Entry for Exclusions” on page 193.

You can configure a path to a particular folder or file along with the host. The protocol, port, and the request parameters are simply ignored in the URL. If a path is configured, then the exclusion is recursively applied to all subfolders and files. For instance, if **Host** is set to **webmail.sonicwall.com/exchange**, then all files and folders under **exchange** are also excluded.

Step 4 Click **Add** to move the host name into the list box.



Step 5 Repeat Step 3 and Step 4 to add more hosts to this exclusion.

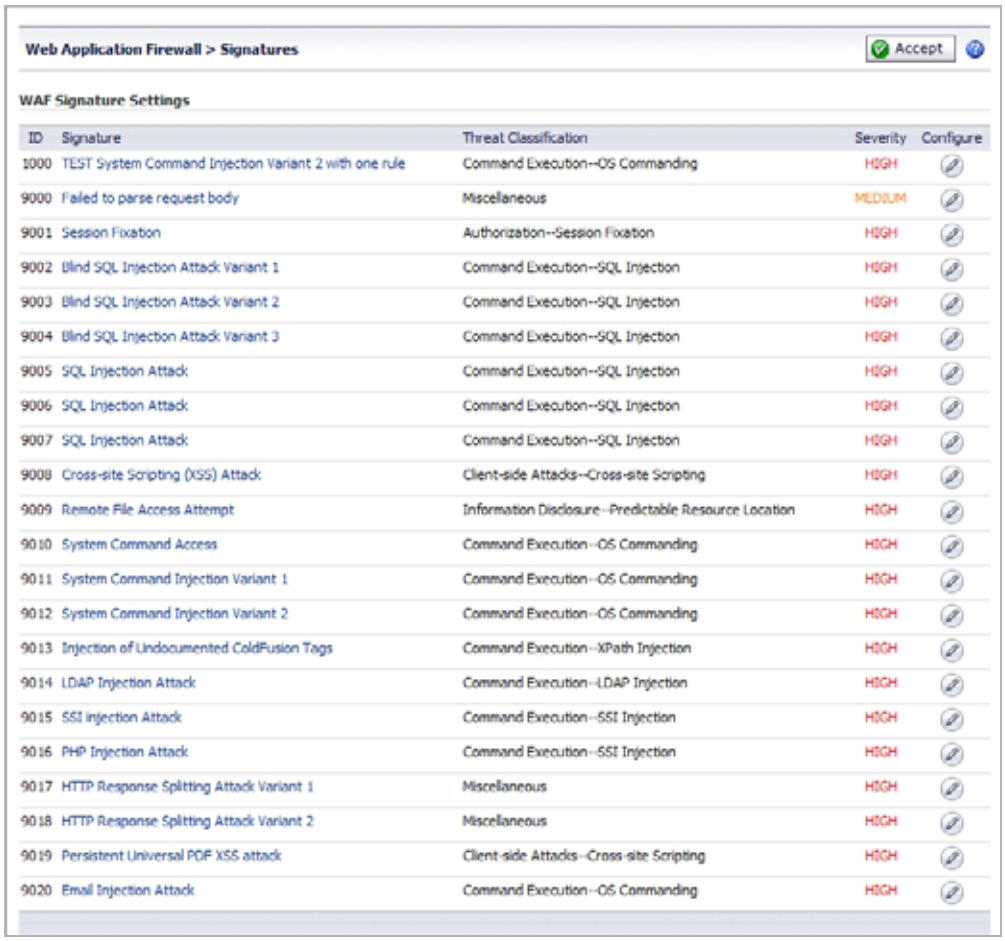
Step 6 Click **Apply**. SonicOS SSL VPN verifies that the host entry is valid and prompts you to restart the SSL-VPN appliance.

Step 7 Click **OK** in the confirmation dialog box to restart the appliance and apply the updated settings.

Configuring Web Application Firewall Signature Actions

The Web Application Firewall > Signatures page allows you to configure custom handling or exclusion of certain hosts on a per-signature basis. In SonicOS SSL VPN 4.0 and higher, you can use signature-based exclusions to apply exclusions for all hosts for each signature.

You can also revert back to using the global settings for the signature group to which this signature belongs without losing the configuration details of existing exclusions.



On the Web Application Firewall > Settings page, global settings must be set to either Prevent All or
Detect All for the Signature Group to which the specific signature belongs. If neither is set, that Signature Group is globally disabled and cannot be modified on a per-signature basis. See “Enabling Web Application Firewall and Configuring Settings” on page 187.

See the following sections:

- “Configuring Signature Based Custom Handling and Exclusions” on page 191
- “Reverting a Signature to Global Settings” on page 193
- “Removing a Host from a Per-Signature Exclusion” on page 193

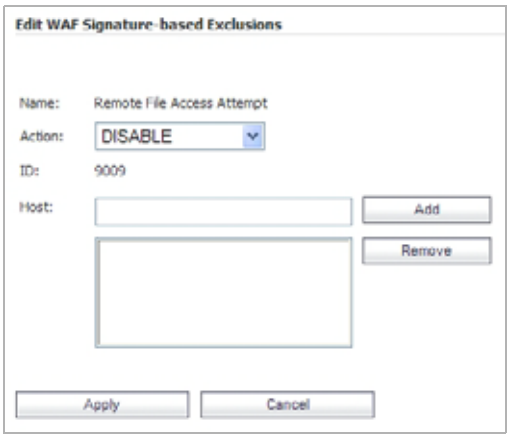
Configuring Signature Based Custom Handling and Exclusions

You can disable inspection for a signature in traffic to an individual host, or for all hosts. You can also change the handling of detected threats for an individual host or for all hosts. If the signature group to which the signature belongs is set globally to Detect All, you can raise the level of protection to Prevent for the configured hosts. If no hosts are configured, the action is applied to the signature itself and acts as a global setting for all hosts. This change will block access to a host when the attack signature is detected. Similarly, you can lower the level of protection to Detect if the associated signature group is globally set to Prevent All.

Note For signature based customization to take effect, the signature group of the modified signature must be globally enabled for either prevention or detection on the Web Application Firewall > Settings page.

To configure one or more hosts with an exclusion from inspection for a signature, or to configure custom handling when Web Application Firewall detects a specific signature for one or more hosts, perform the following steps:

Step 1 On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change. The **Edit WAF Signature-based Exclusions** screen displays.



Step 2 In the Edit WAF Signature-based Exclusions screen, select one of the following actions from the **Action** drop-down list:

- **DISABLE** – Disable Web Application Firewall inspections for this signature in traffic from hosts listed in this exclusion
- **DETECT** – Detect and log threats matching this signature from hosts listed in this exclusion, but do not block access to the host
- **PREVENT** – Log and block host access for threats matching this signature from hosts listed in this exclusion

Step 3 To apply this action globally to all hosts, leave the **Host** field blank. To apply this action to an individual host, type the host entry as it appears in the bookmark or offloaded application into the **Host** field. This can be a host name or an IP address. To determine the correct host entry for this exclusion, see "Determining the Host Entry for Exclusions" on page 193.

You can configure a path to a particular folder or file along with the host. The protocol, port, and the request parameters are simply ignored in the URL. If a path is configured, then the exclusion is recursively applied to all subfolders and files. For instance, if **Host** is set to **webmail.sonicwall.com/exchange**, then all files and folders under **exchange** are also excluded.

Step 4 If you specified a host, click **Add** to move the host name into the list box.

Step 5 If you want to apply this action to additional individual hosts, repeat Step 3 and Step 4 to add more hosts to this exclusion.

Step 6 Click **Apply**. If the Host list contains host entries, SonicOS SSL VPN verifies that each host entry is valid. If no hosts were specified, a dialog box confirms that this is a global action to be applied to the signature itself.

Step 7 Click **OK** in the confirmation dialog box.

Step 8 Click **Apply** on the Web Application Firewall > Signatures page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests will continue to use the old settings until they are terminated.

Reverting a Signature to Global Settings

You can revert to using global signature group settings for a signature that was previously configured with an exclusion, without losing the configuration. This allows you to leave the host names in place in case you need to re-enable the exclusion.

To revert to using global signature group settings for a signature, perform the following steps:

Step 1 On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change.

Step 2 In the Edit WAF Signature-based Exclusions screen, select **INHERIT GLOBAL** from the **Action** drop-down list.

Step 3 The **Host** field may be blank if global settings were previously applied to this signature. To revert to global signature settings for all hosts, leave the **Host** field blank. To apply this action to one or more individual hosts, leave these host entries in the **Host** field and remove any host entries that are not to be reverted.

Step 4 Click **Apply**. SonicOS SSL VPN verifies that each host entry is valid.

Step 5 Click **OK** in the confirmation dialog box.

Step 6 Click **Apply** on the Web Application Firewall > Signatures page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests will continue to use the old settings until they are terminated.

Removing a Host from a Per-Signature Exclusion

To remove a host from a configured exclusion for a signature, perform the following steps:

Step 1 On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change.

Step 2 Select the host entry in the list box under the Host field, and then click **Remove**.

Step 3 Repeat Step 2 to remove other listed hosts, if desired.

Step 4 Click **Apply**. SonicOS SSL VPN verifies that each host entry is valid.

Step 5 Click **OK** in the confirmation dialog box.

Step 6 Click **Apply** on the Web Application Firewall > Signatures page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests will continue to use the old settings until they are terminated.

Determining the Host Entry for Exclusions

When configuring an exclusion, either globally or per-signature, you must provide the host name or IP address. The affected hosts must match the host names used in your HTTP(S) bookmarks and Citrix bookmarks, and the virtual host domain name configured for an offloaded Web application.

For a description of how to determine the correct host name, see the following sections:

- “Viewing the Host Entry in a Bookmark” on page 194
- “Viewing the Host Entry in an Offloaded Application” on page 194

Viewing the Host Entry in a Bookmark

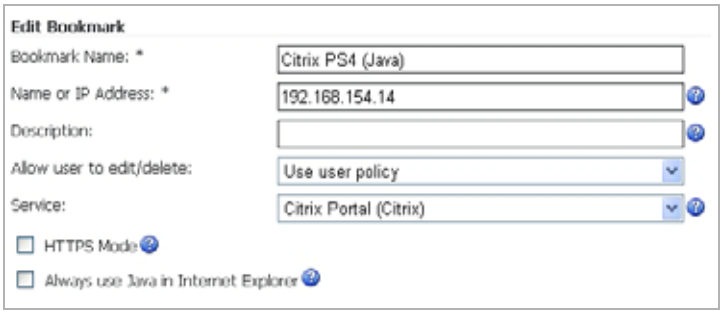
You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the bookmark.

To view the host entry in a bookmark, perform the following steps:

Step 1 Navigate to the Virtual Office page, and click **Show Edit Controls** above the list of bookmarks.

Step 2 Click the Edit button for the bookmark.

Step 3 In the Edit Bookmark screen, view the host entry in the **Name or IP Address** field.



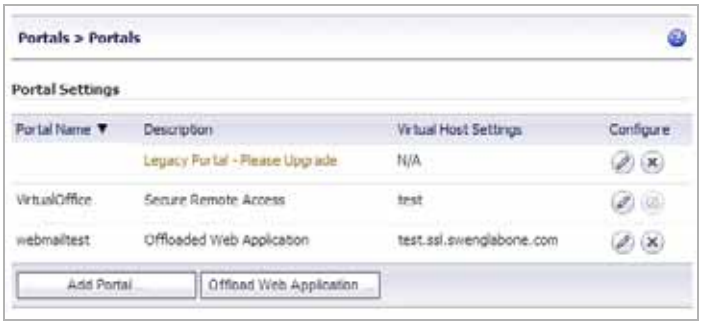
Step 4 Click **Cancel**.

Viewing the Host Entry in an Offloaded Application

You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the offloaded application. In an offloaded application, you will use the virtual host domain name.

To view the virtual host domain name in an offloaded application, perform the following steps:

Step 1 Navigate to the Portals > Portals page and click the Configure button next to the offloaded application.



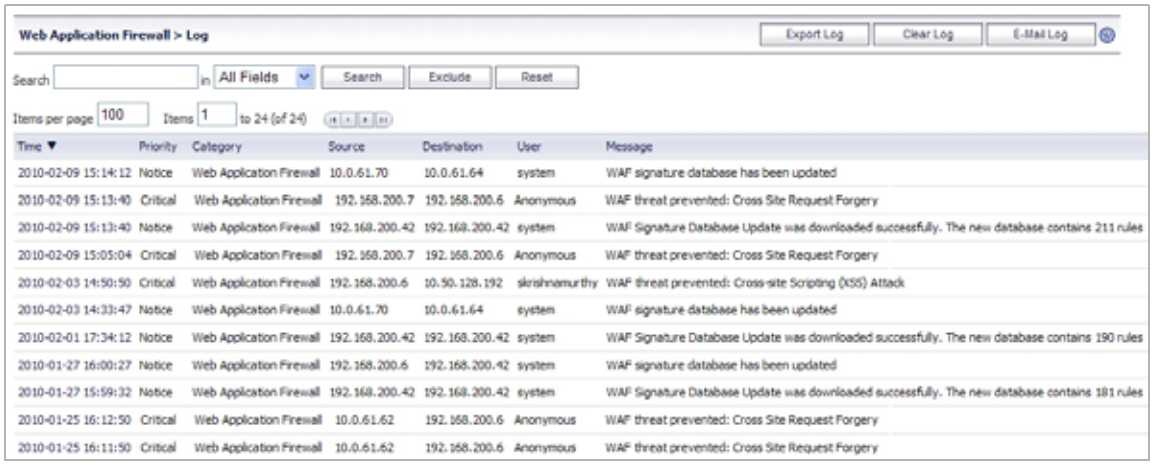
Step 2 In the Edit Portal screen, click the **Virtual Host** tab.

Step 3 View the host entry for your exclusion in the **Virtual Host Domain Name** field.

Step 4 Click **Close**.

Using Web Application Firewall Logs

The Web Application Firewall > Log page provides a number of functions, including a flexible search mechanism, and the ability to export the log to a file or email it. The page also provides a way to clear the log. Clicking on a log entry displays more information about the event.



See the following sections:

Searching the Log

You can search for a value contained in a certain column of the log table, and can also search for log entries that do **not** contain the specified value.

To view and search Web Application Firewall log files, perform the following steps:

Step 1 On the Web Application Firewall > Log page, type the value to search for into the **Search** field.

Step 2 Select the column in which to search from the drop-down list to the right of the Search field.

Step 3 Do one of the following:

- To start searching for log entries containing the search value, click **Find**.
- To start searching for log entries that do not contain the search value, click **Exclude**.
- To clear the Search field, set the drop-down list back to the default (Time), and display the first page of log entries, click **Reset**.

Controlling the Log Pagination

To adjust the number of entries on the log page and display a different range of entries, perform the following steps:

Step 1 On the Web Application Firewall > Log page, enter the number of log entries that you want on each page into the **Items per Page** field. The Log page display changes to show the new number of entries.

Step 2 To view the log entries beginning at a certain number, type the starting number into the **Item** field and press **Enter** on your keyboard.

Step 3 To view the first page of log entries, click the left-most button in the arrow control pad.

Step 4 To view the previous page of log entries, click the left arrow in the arrow control pad.

Step 5 To view the next page of log entries, click the right arrow in the arrow control pad.

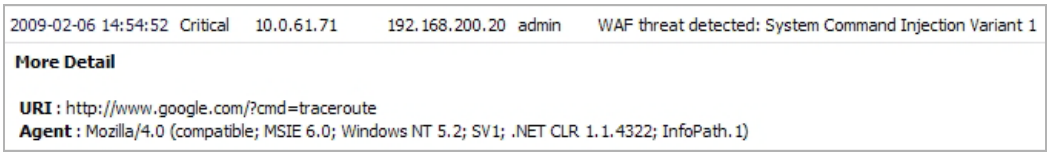
Step 6 To view the last page of log entries, click the right-most button in the arrow control pad.

Viewing Log Entry Details

The log entry details vary with the type of log entry. The URI (Uniform Resource Indicator) is provided along with the command for detected threats. Information about the agent that caused the event is also displayed. For an explanation of the rather cryptic Agent string, the following Wikipedia page provides a description and links to external sites that can analyze any user agent string: http://en.wikipedia.org/wiki/User_agent

To view more details about an individual log entry, perform the following steps:

Step 1 On the Web Application Firewall > Log page, click anywhere on the log entry that you want to view. The details are displayed directly beneath the entry.



Step 2 To collapse the details for a log entry, click again on the entry.

Exporting and Emailing Log Files

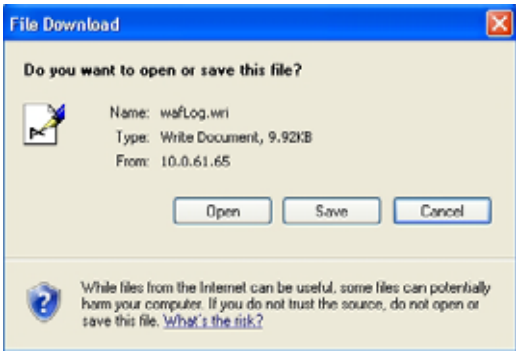
You can export the current contents of the Web Application Firewall log to a file, or email the log contents by using the buttons in the top right corner of the Web Application Firewall > Log page.

Exported files are saved with a **.wri** file name extension, and open with Wordpad, by default.

Emailed files are automatically sent to the address configured on the Log > Settings page of the SSL-VPN management interface. If no address is configured, the Status line at the bottom of the browser will display an error message when you click the **E-Mail Log** button on the Web Application Firewall > Log page.

To export or email the log, perform the following steps:

Step 1 To export the log contents, click the **Export** button in the top right corner of the Web Application Firewall > Log page. The File Download dialog box is displayed.



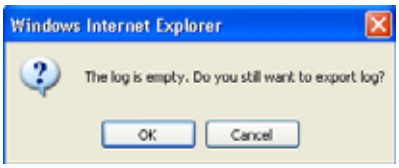
Step 2 In the File Download dialog box, do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, then browse to the folder where you want to save the file and click **Save**.

Step 3 To email the log contents, click the **E-Mail Log** button in the top right corner of the Web Application Firewall > Log page. The log contents are emailed to the address specified in the Log > Settings page.

Clearing the Log

You can remove all entries from the Web Application Firewall log on the Web Application Firewall > Log page. The entries on the page are removed, and any attempt to export or email the log file while it is still empty will cause a confirmation dialog box to display.



To clear the Web Application Firewall log, perform the following:

Step 1 On the top right corner of the Web Application Firewall > Log page, click **Clear**.

Note The page and log are immediately cleared without asking for confirmation.

Verifying and Troubleshooting Web Application Firewall

You can verify the correct configuration of Web Application Firewall by viewing the Web Application Firewall > Status page. This page displays statistics on all threats detected since Web Application Firewall was activated. With normal use and exposure to the Internet, you should begin to see statistics within a day of activation.

You can also find helpful information in both the Log > View page and Web Application Firewall > Log page. This section lists some of the relevant log messages and provides an explanation or suggestions for actions in those cases.

Log > View Messages

The following messages can be viewed from the Log > View page:

- License Manager SSL connection failed - Restart appliance may be necessary

  Test the connectivity to **licensemanager.sonicwall.com** from the System > Diagnostics page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.

- License Manager Failed to resolve host. Check DNS.

  Test the connectivity to **licensemanager.sonicwall.com** from the System > Diagnostics page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.

- License Manager Peer Identity failed - Check certs and time

  The License Manager server or the signature database server may not have a valid SSL Certificate.

- License Manager Reset called

  The device licenses have been reset. Navigate to the System > Licenses page to activate, upgrade or renew licenses.

Web Application Firewall > Log and Log > View Messages

The following messages can be viewed from the Web Application Firewall > Log page and the Log > View page:

- WAF signature database update failed: No signatures were found in the update

  The download for the database update completed, but no suitable signatures were found in the database.

- WAF signature database update failed: Old signature timestamp found in the update

  The timestamp found in the database update from the License Manager is older than what was originally advertised before the download for the update started.

- WAF signature database update failed: Error occurred while processing the update

  There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.

- WAF signature database update failed: Error occurred while downloading the WAF signature database update

  There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.

- WAF signature database update was downloaded successfully. The new database contains <num> rules

  Signature database download was successful. The new database contains <num> number of rules. A rule is an internal property which will be used by SonicWALL to determine how many signatures were downloaded.

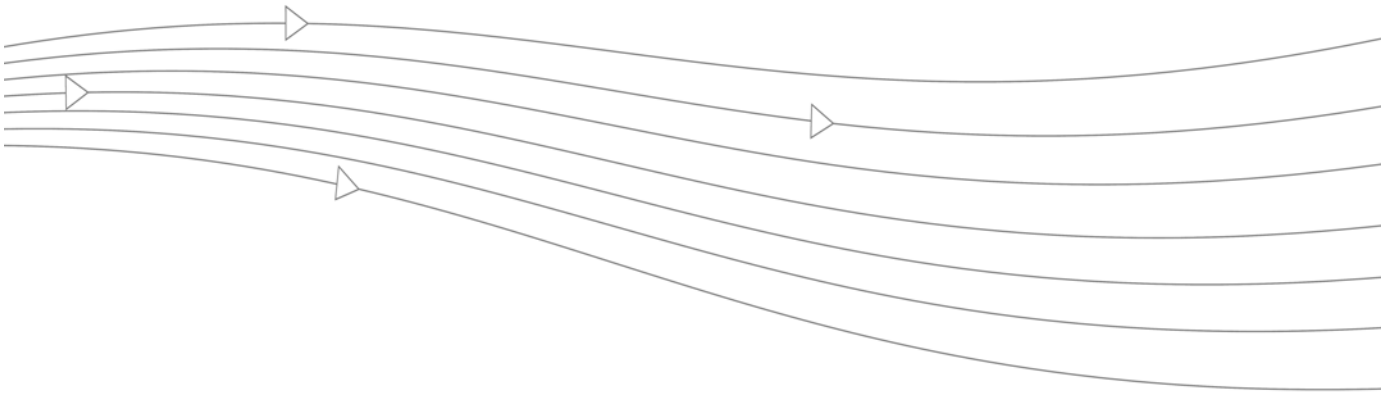
Note You can select the **Apply Signature Updates Automatically** option on the Web Application Firewall > Settings page to apply new signatures automatically. If this option is not selected, you must click the **Apply** button that appears on the Web Application Firewall > Status page after a successful download. After the database has been successfully applied, all of the signatures within the new database can be found on the Web Application Firewall > Signatures page.

- WAF signature database has been updated

  The signature database update was applied after the administrator clicked on the **Apply** button on the Web Application Firewall > Status page.

- WAF engine is being started with the factory default signature database

  The Web Application Firewall engine will be using the factory default signature database for traffic inspection. This may imply that no new signatures were found since the firmware update. If an attempt to download is revealed in the logs earlier, then this message could also imply that the update could not be processed successfully due to database errors and as a precautionary measure the factory default database has been used.



Chapter 9: Users Configuration

This chapter provides information and configuration tasks specific to the **Users** pages on the SonicWALL SSL VPN Web-based management interface, including access policies and bookmarks for the users and groups. Policies provide you access to the different levels of objects defined on your SonicWALL SSL-VPN appliance. This chapter contains the following sections:

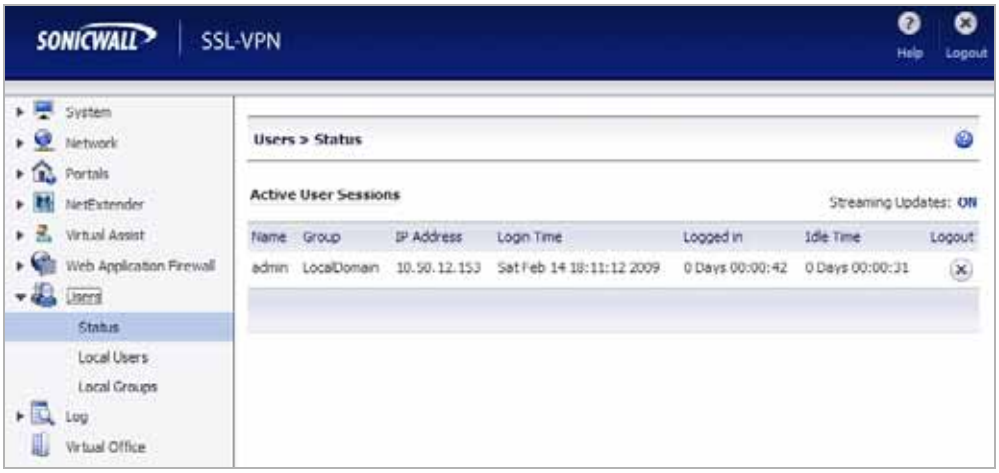
Users > Status

The **Users > Status** page provides information about users and administrators who are currently logged into the SonicWALL SSL-VPN appliance. This section provides general information about how SonicWALL SSL VPN manages users through a set of hierarchical policies.

This section contains the following sub-sections:

- "Access Policies Concepts" section on page 203
- "Access Policy Hierarchy" section on page 203

Figure 26 Users > Status Page



When **Streaming Updates** is set to **ON**, the **Users > Status** page content is automatically refreshed so that the page always displays current information. Toggle to **OFF** by clicking **ON**.

The **Active User Sessions** table displays the current users or administrators logged into SonicWALL SSL VPN. Each entry displays the name of the user, the group in which the user belongs, the IP address of the user, and a time stamp indicating when the user logged in. An administrator may terminate a user session and log the user out by clicking the Logout icon at the right of the user row. The **Active User Session** table includes the following information:

Table 12 Active User Information

Column	Description
Name	A text string that indicates the ID of the user.
Group	The group to which the user belongs.
IP Address	The IP address of the workstation on which the user is logged into.
Login Time	The time when the user first established connection with the SonicWALL SSL-VPN appliance expressed as day, date, and time (HH:MM:SS).
Logged In	The amount of time since the user first established a connection with the SonicWALL SSL-VPN appliance expressed as number of days and time (HH:MM:SS).
Idle Time	The amount of time the user has been in an inactive or idle state with the SonicWALL SSL-VPN appliance.
Logout	Displays an icon that enables you to log the user out of the appliance.

Access Policies Concepts

The SonicWALL SSL VPN Web-based management interface provides granular control of access to the SonicWALL SSL-VPN appliance. Access policies provide different levels of access to the various network resources that are accessible using the SonicWALL SSL-VPN appliance. There are three levels of access policies: global, groups, and users. You can block and permit access by creating access policies for an IP address, an IP address range, all addresses, or a network object.

Access Policy Hierarchy

An administrator can define user, group and global policies to predefined network objects, IP addresses, address ranges, or all IP addresses and to different SonicWALL SSL VPN services. Certain policies take precedence.

The SonicWALL SSL VPN policy hierarchy is:

- User policies take precedence over group policies
- Group policies take precedence over global policies
- If two or more user, group or global policies are configured, the most specific policy takes precedence

For example, a policy configured for a single IP address takes precedence over a policy configured for a range of addresses. A policy that applies to a range of IP addresses takes precedence over a policy applied to all IP addresses. If two or more IP address ranges are configured, then the smallest address range takes precedence. Hostnames are treated the same as individual IP addresses.

Network objects are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network object.

For example:

- Policy 1: A Deny rule has been configured to block all services to the IP address range 10.0.0.0 - 10.0.0.255
- Policy 2: A Deny rule has been configured to block FTP access to 10.0.1.2 - 10.0.1.10
- Policy 3: A Permit rule has been configured to allow FTP access to the predefined network object, FTP Servers. The FTP Servers network object includes the following addresses: 10.0.0.5 - 10.0.0.20. and ftp.company.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access:

- An FTP server at 10.0.0.1, the user would be blocked by Policy 1
- An FTP server at 10.0.1.5, the user would be blocked by Policy 2
- An FTP server at 10.0.0.10, the user would be granted access by Policy 3. The IP address range 10.0.0.5 - 10.0.0.20 is more specific than the IP address range defined in Policy 1.
- An FTP server at ftp.company.com, the user would be granted access by Policy 3. A single host name is more specific than the IP address range configured in Policy 2.

Note In this example, the user would not be able to access ftp.company.com using its IP address 10.0.1.3. The SSL VPN policy engine does not perform reverse DNS lookups.

Tip When using Citrix bookmarks, in order to restrict proxy access to a host, a Deny rule must be configured for both Citrix and HTTP services.

Users > Local Users

This section provides an overview of the **Users > Local Users** page and a description of the configuration tasks available on this page.

For global configuration settings, see the "Global Configuration" section on page 246.

Users > Local Users Overview

The **Users > Local Users** page allows the administrator to add and configure users.

Figure 27 Users > Local Users Page

Local Users

The Local Users section allows the administrator to add and configure users by specifying a user name, selecting a group/domain, creating and confirming password, and selecting user type (user or administrator).

Note Users configured to use RADIUS, LDAP, NT Domain or Active Directory authentication do not require passwords because the external authentication server will validate user names and passwords.

Tip When a user is authenticated using RADIUS and Active Directory, an External User within the Local User database is created, however, the administrator will not be able to change the group for this user. If you want to specify different policies for different user groups when using RADIUS or Active Directory, the administrator will need to create the user manually in the Local User database.

Adding a Local User

To create a new local user, perform the following steps:

Step 1 Navigate to the **Users** > **Local Users** page and click **Add User**. The **Add Local User** dialog box is displayed.

Step 2 In the **Add Local User** dialog box, enter the username for the user in the **User Name** field. This will be the name the user will enter in order to log into the SonicWALL SSL VPN user portal.

Step 3 Select the name of the group to which the user belongs in the **Group/Domain** drop-down list.

Step 4 Type the user password in the **Password** field.

Step 5 Retype the password in the **Confirm Password** field to verify the password.

Note When logging into the portal, the user name is not case-sensitive, but the password and domain are case-sensitive.

Step 6 From the **User Type** drop-down list, select a user type option. The available user types are **User**, **Administrator**, **Read-only Administrator**.

A Read-only Administrator is able to view the management interface but may not modify the configuration.

Tip If the selected group is in a domain that uses external authentication, such as Active Directory, RADIUS, NT Domain or LDAP, then the **Add User** window will close and the new user will be added to the **Local Users** list.

Step 7 Click **Add** to update the configuration. Once the user has been added, the new user will be added to the **Local Users** window.

Note Entering RADIUS, LDAP, NT and Active Directory user names is only necessary if you wish to define specific policies or bookmarks per user. If users are not defined in the SonicWALL SSL-VPN appliance, then global policies and bookmarks will apply to users authenticating to an external authentication server. When working with external (non-LocalDomain) users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SonicWALL SSL-VPN configuration files. Bookmarks must be stored on the SonicWALL SSL-VPN 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, SonicWALL SSL VPN will automatically create a corresponding local user entity when an external domain user creates a personal bookmark so that it may store the bookmark information.

Removing a User

To remove a user, navigate to **Users > Local Users** and click the delete icon next to the name of the user that you wish to remove. Once deleted, the user will be removed from the **Local Users** window.

Editing User Settings

To edit a user's attributes, navigate to the **Users** > **Local Users** window and click the Configure icon next to the user whose settings you want to configure. The **Edit User Settings** window displays.

The **Edit User Settings** window has six tabs as described in the following table:

Tab	Description
General	Enables you to create a password and an inactivity timeout, and specify Single Sign-On settings for automatic login to bookmarks for this user.
Portal	Enables you to enable, disable, or use group settings on this portal for NetExtender, File Shares, Virtual Assist, and Bookmark settings.
Nx Settings	Enables you to specify a NetExtender client address range, including for IPv6, and to configure client settings. (Not supported on the SSL-VPN 200 appliance.)
Nx Routes	Enables you to specify Tunnel All mode and NetExtender client routes. (Not supported on the SSL-VPN 200 appliance.)
Policies	Enables you to create access policies that control access to resources from user sessions on the appliance.
Bookmarks	Enables you to create user-level bookmarks for quick access to services.
Login Policies	Enables you to create user login policies, including policies for specific source IP addresses and policies for specific client browsers. You can disable the user's login, require One Time Passwords, and specify client certificate enforcement.

If the user authenticates to an external authentication server, then the **User Type** and **Password** fields will not be shown. The password field is not configurable because the authentication server validates the password. The user type is not configurable because the SonicWALL SSL-VPN appliance only allows users that authenticate to the internal user database to have administrative privileges. Also, the user type **External** will be used to identify the local user instances that are auto-created to correspond to externally authenticating users.

See the following sections for a description of the configuration options on each tab of the **Edit User Settings** window:

- "Modifying General User Settings" section on page 207
- "Modifying Portal Settings" section on page 209
- "Modifying User NetExtender Settings" section on page 209
- "Modifying NetExtender Client Routes" section on page 209
- "Adding User Policies" section on page 210
- "Adding or Editing User Bookmarks" section on page 216
- "Configuring Login Policies" section on page 224

Modifying General User Settings

The **General** tab provides configuration options for a user's password, inactivity timeout value, and bookmark single sign-on (SSO) control. Table 13 provides detailed information about application-specific support of SSO, global/group/user policies and bookmark policies.

Table 13 Application Support

Application	Supports SSO	Global/Group/User Policies	Bookmark Policies
Terminal Services (RDP - Active X)	Yes	Yes	Yes
Terminal Services (RDP - Java)	Yes	Yes	Yes
Virtual Network Computing (VNC)	No	No	No
File Transfer Protocol (FTP)	Yes	Yes	Yes
Telnet	No	No	No
Secure Shell (SSH)	No	No	No
Web (HTTP)	Yes	No	No
Secure Web (HTTPS)	Yes	No	No
File Shares (CIFS)	Yes	Yes	Yes
Citrix Portal (Citrix)	No	Yes	No

Single sign-on (SSO) in SonicWALL SSL VPN supports the following applications:

- RDP - Active X
- RDP - Java
- FTP
- HTTP
- HTTPS
- CIFS

Note SSO cannot be used in tandem with two-factor authentication methods.

To modify general user settings, perform the following tasks:

Step 1 In the left-hand column, navigate to the **Users** > **Local Users**.

Step 2 Click the configure icon next to the user you want to configure. The **General** tab of the **Edit User Settings** window displays. The **General** tab displays the following non-configurable fields: **User Name**, **In Group**, and **In Domain**. If information supplied in these fields need to be modified, then remove the user as described in "Removing a User" section on page 206 and add the user again.

Step 3 To set or change the user password, type the password in the **Password** field. Re-type it in the **Confirm Password** field.

Step 4 To set the inactivity timeout for the user, meaning that they will be signed out of the Virtual Office after the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field. The timeout value also controls the number of minutes that a one-time password remains valid, when One Time Passwords are configured for a user.

Note The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

Step 5 To allow users to edit or delete user-owned bookmarks, select **Allow** from the **Allow user to edit/delete bookmarks** drop-down menu. To prevent users from editing or deleting user-owned bookmarks, select **Deny**. To use the group policy, select **Use group policy**.

Note Users cannot edit or delete group and global bookmarks.

Step 6 To allow users to add new bookmarks, select **Allow** from the **Allow user to add bookmarks** drop-down menu. To prevent users from adding new bookmarks, select **Deny**. To use the group policy, select **Use group policy**.

Note Bookmark modification controls provide custom access to predetermined sources, and can prevent users from needing support.

Step 7 Under **Single Sign-On Settings**, select one of the following options from the Use SSL VPN account credentials to log into bookmarks drop-down menu:

- **Use Group Policy**: Select this option to use the group policy settings to control single sign-on (SSO) for bookmarks.
- **User-controlled**: Select this option to allow users to enable or disable single sign-on (SSO) for bookmarks.
- **Enabled**: Select this option to enable single sign-on for bookmarks.
- **Disabled**: Select this option to disable single sign-on for bookmarks.

Note SSO modification controls provide enhanced security and can prevent or allow users to utilize different login credentials. With SSO enabled, the user's login name and password are supplied to the backend server for many of the services. For Fileshares, the domain name that the user belongs to on the device is passed to the server. For other services, the server may be expecting the username to be prefixed by the domain name. In this instance, SSO will fail and the user will have to login with the domain-prefixed username. In some instances, a default domain name can be configured at the server to allow SSO to succeed.

Step 8 Click **OK** to save the configuration changes

Modifying Portal Settings

The **Portal** tab provides configuration options for portal settings for this user.

To configure portal settings for this user, perform the following steps:

Step 1 On the **Portal** tab under **Portal Settings**, select one of the following portal settings for this user:

- **Use group setting** – The setting defined in the group to which this user belongs will be used to determine if the portal feature is enabled or disabled. Group settings are defined by configuring the group in the **Users > Local Groups** page.
- **Enabled** – Enable this portal feature for this user.
- **Disabled** – Disable this portal feature for this user.

You can configure one of the above settings for each of the following portal features:

- **NetExtender**
- **Launch NetExtender after login**
- **File Shares**
- **Virtual Assist**
- **Allow User to Add Bookmarks**
- **Allow User to Edit/Delete Bookmarks** – Applies to user-owned bookmarks only.

Step 2 Click **OK**.

Modifying User NetExtender Settings

Note Group NetExtender settings are not supported on the SonicWALL SSL-VPN 200 appliance.

The **Nx Settings** tab provides configuration options for NetExtender client address ranges and other client settings. For procedures on modifying NetExtender User settings, see the "NetExtender > Client Settings" section on page 161.

Modifying NetExtender Client Routes

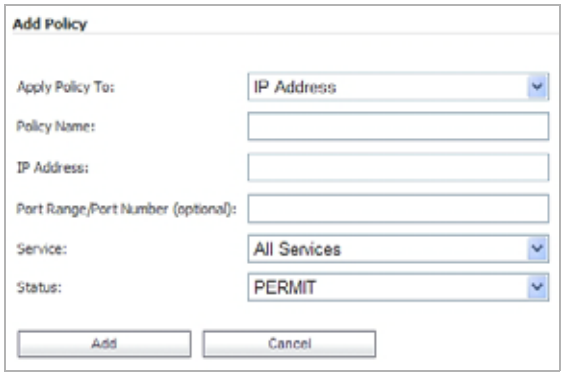
Note Group NetExtender routes are not supported on the SonicWALL SSL-VPN 200 appliance.

The **Nx Routes** tab provides configuration options for NetExtender client routes. For procedures on modifying NetExtender client route settings, see the "NetExtender > Client Routes" section on page 163.

Adding User Policies

The **Policies** tab provides policy configuration options. To add a user access policy, perform the following steps:

Step 1 On the **Policies** tab, click **Add Policy**. The **Add Policy** dialog box is displayed.



Step 2 In the **Apply Policy To** drop-down list, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. On SonicWALL SSL-VPN models 2000 and higher, you can also select an individual IPv6 host, a range of IPv6 addresses, or all IPv6 addresses. The **Add Policy** dialog box changes depending on what type of object you select in the **Apply Policy To** drop-down list.

Note These SonicWALL SSL VPN policies apply to the destination address(es) of the SonicWALL SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SonicWALL SSL VPN gateway with a policy created on the **Policies** tab. However, it is possible to control source logins by IP address with a login policy created on the user's **Login Policies** tab. For more information, refer to "Configuring Login Policies" section on page 224.

- **IP Address** - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IP Address" section on page 211.
- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IP Address Range" section on page 211.
- **All Addresses** - If your policy applies to all IPv4 addresses, you do not need to enter any IP address information. See "Adding a Policy for All Addresses" section on page 212.
- **Network Object -** If your policy applies to a predefined network object, select the name of the object from the **Network Object** drop-down list. A port or port range can be specified when defining a Network Object. See "Configuring Network Objects" section on page 101
- **Server Path** - If your policy applies to a server path, select one of the following radio buttons in the **Resource** field:
  - **Share (Server path)** - When you select this option, type the path into the **Server Path** field.
  - **Network (Domain list)**
  - **Servers (Computer list)**

See "Setting File Shares Access Policies" section on page 212.

- **URL Object** - If your policy applies to a predefined URL object, type the URL into the **URL** field. See "Adding a Policy for a URL Object" section on page 213.
- **IPv6 Address** - On SonicWALL SSL-VPN models 2000 and higher, if your policy applies to a specific host, enter the IPv6 address of the local host machine in the **IPv6 Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IPv6 Address" section on page 215.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See "Adding a Policy for an IPv6 Address Range" section on page 215.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See "Adding a Policy for All IPv6 Addresses" section on page 215.

Step 3 Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

Step 4 Select **PERMIT** or **DENY** from the **Status** drop-down list to either permit or deny SonicWALL SSL VPN connections for the specified service and host machine.

Tip When using Citrix bookmarks, in order to restrict proxy access to a host, a DENY rule must be configured for both Citrix and HTTP services.

Step 5 Click **Add** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Edit User Settings** window.

The user policies are displayed in the **Current User Policies** table in the order of priority, from the highest priority policy to the lowest priority policy.

Adding a Policy for an IP Address

Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy...**

Step 5 In the **Apply Policy to** field, click the IP Address option.

Step 6 Define a name for the policy in the **Policy Name** field.

Step 7 Type an IP address in the **IP Address** field.

Step 8 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

Step 9 In the **Service** drop-down list, click on a service object.

Step 10 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 11 Click **Add**.

Adding a Policy for an IP Address Range

Step 1 In the **Apply Policy to** field, click the IP Address Range option.

Step 2 Define a name for the policy in the **Policy Name** field.

Step 3 Type a starting IP address in the **IP Network Address** field.

Step 4 Type a subnet mask value in the **Subnet Mask** field in the form 255.255.255.0.

Step 5 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

Step 6 In the **Service** drop-down list, click on a service option.

Step 7 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 8 Click **Add**.

Adding a Policy for All Addresses

Step 1 In the **Apply Policy to** field, select the **All Addresses** option.

Step 2 Define a name for the policy in the **Policy Name** field.

Step 3 The **IP Address Range** field is read-only, specifying All IP Addresses.

Step 4 In the **Service** drop-down list, click on a service option.

Step 5 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 6 Click **Add**.

Setting File Shares Access Policies

To set file share access policies, perform the following steps:

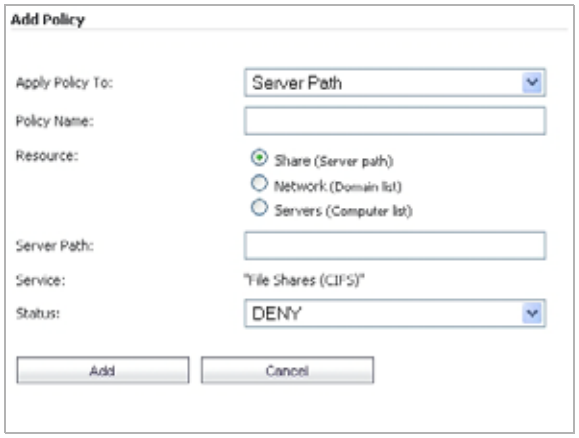
Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy**.

Step 5 Select **Server Path** from the **Apply Policy To** drop-down list.



Step 6 Type a name for the policy in the **Policy Name** field.

Step 7 Select the **Share** radio button in the **Resource** field.

Step 8 Type the server path in the **Server Path** field.

Step 9 From the **Status** drop-down list, select **PERMIT** or **DENY**.

Note For information about editing policies for file shares, for example, to restrict server path access, refer to "Adding a Policy for a File Share" on page 213.

Step 10 Click **Add.**

Adding a Policy for a File Share

To add a file share access policy, perform the following steps:

Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy...**

Step 5 Select **Server Path** from the **Apply Policy To** drop-down list.

Step 6 Type a name for the policy in the **Policy Name** field.

Step 7 In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername\share\path*. The prefixes \\, //, \ and / are acceptable.

Note Share and path provide more granular control over a policy. Both are optional.

Step 8 Select **PERMIT** or **DENY** from the **Status** drop-down list.

Step 9 Click **Add**.

Adding a Policy for a URL Object

To create object-based HTTP or HTTPS user policies, perform the following steps:

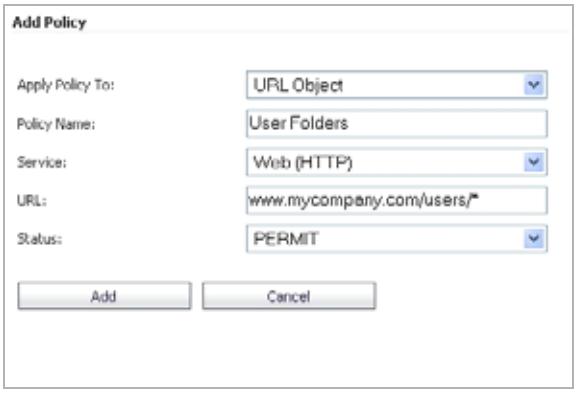
Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy**.

Step 5 In the **Apply Policy To** drop-down menu, select the **URL Object** option.



Step 6 Define a name for the policy in the **Policy Name** field.

Step 7 In the **Service** drop-down list, choose either **Web (HTTP)** or **Secure Web (HTTPS)**.

Step 8 In the **URL** field, add the URL string to be enforced in this policy.

Note In addition to standard URL elements, the administrator may enter port, path and wildcard elements to the URL field. For more information on using these additional elements, see "Policy URL Object Field Elements" section on page 214.

If a path is specified, the URL policy is recursive and applies to all subdirectories. If, for example "www.mycompany.com/users/*" is specified, the user is permitted access to any folder or file under the "www.mycompany.com/users/" folder.

Step 9 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 10 Click **Add**.

Policy URL Object Field Elements

When creating an HTTP/HTTPS policy, the administrator must enter a valid host URL in the URL field. In addition, the administrator may enter port, path and wildcard elements to this field.The following chart provides an overview of standard URL field elements:

Element	Usage
Host	Can be a hostname that should be resolved or an IP address. Host information has to be present.
Port	If port is not mentioned, then all ports for that host are matched. Specify a specific port or port range using digits [0-9], and/or wildcard elements. Zero "0" must not be used as the first digit in this field. The least possible number matching the wildcard expression should fall within the range of valid port numbers i.e. [1-65535].
Path	This is the file path of the URL along with the query string. A URL Path is made of parts delimited by the file path separator '/'. Each part may contain wildcard characters. The scope of the wildcard characters is limited only to the specific part contained between file path separators.
Usernames	%USERNAME% is a variable that matches the username appearing in a URL requested by a user with a valid session. Especially useful if the policy is a group or a global policy.
Wildcard Characters	The following wildcard characters are used to match one or more characters within a port or path specification. ***** – Matches one or more characters in that position. **^** – Matches exactly one character in the position. **[!<character set>]** – Matches any character in that position not listed in character set. E.g. **[!acd]**, **[!8a0]** **[<range>]** – Matches any character falling within the specified ASCII range. Can be an alphanumeric character. E.g.) **[a-d]**, **[3-5]**, **[H-X]**

Note Entries in the URL field can not contain ("http://", "https://") elements. Entries can also not contain fragment delimiters such as "#".

Adding a Policy for an IPv6 Address

To add a policy for an IPv6 address, perform the following steps:

Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon next to the user you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy...**

Step 5 In the **Apply Policy To** field, click the **IPv6 Address** option.

Step 6 Define a name for the policy in the **Policy Name** field.

Step 7 Type an IPv6 address in the **IPv6 Address** field in the form 2001::1:2:3:4.

Step 8 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

Step 9 In the **Service** drop-down list, click on a service object.

Step 10 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 11 Click **Add**.

Adding a Policy for an IPv6 Address Range

To add a policy for an IPv6 address range, perform the following steps:

Step 1 In the **Apply Policy To** field, click the **IPv6 Address Range** option.

Step 2 Define a name for the policy in the **Policy Name** field.

Step 3 Type a starting IPv6 address in the **IPv6 Network Address** field.

Step 4 Type a prefix value in the **IPv6 Prefix** field, such as 64 or 112.

Step 5 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

Step 6 In the **Service** drop-down list, click on a service option.

Step 7 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 8 Click **Add**.

Adding a Policy for All IPv6 Addresses

To add a policy for all IPv6 addresses, perform the following steps:

Step 1 In the **Apply Policy To** field, select the **All IPv6 Address** option.

Step 2 Define a name for the policy in the **Policy Name** field.

Step 3 The **IPv6 Address Range** field is read-only, specifying All IPv6 Addresses.

Step 4 In the **Service** drop-down list, click on a service option.

Step 5 In the **Status** drop-down list, click on an access action, either **PERMIT** or **DENY**.

Step 6 Click **Add**.

Adding or Editing User Bookmarks

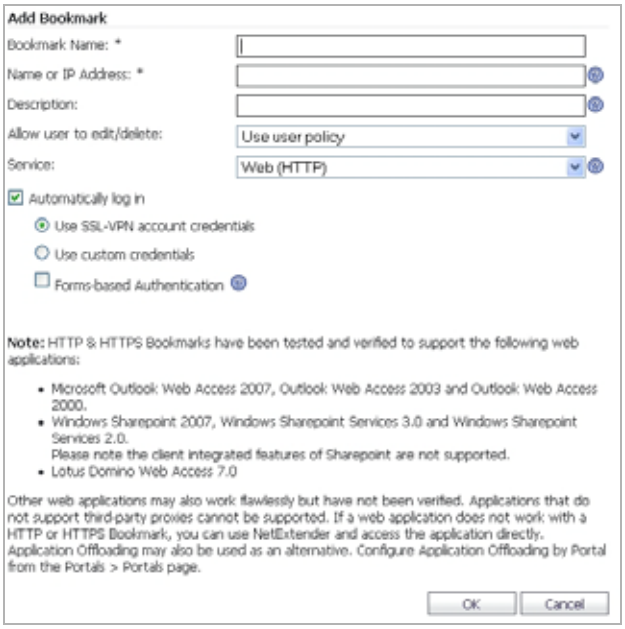
The **Bookmarks** tab provides configuration options to add and edit user bookmarks. In addition to the main procedure below, see the following:

- "Enabling Plugin DLLs" section on page 221
- "Creating a Citrix Bookmark for a Local User" on page 222
- "Creating Bookmarks with Custom SSO Credentials" section on page 223

To define user bookmarks, perform the following steps:

Step 1 In the E**dit User Settings** window, click the **Bookmarks** tab.

Step 2 Click **Add Bookmark**. The **Add Bookmark** window displays.



When user bookmarks are defined, the user will see the defined bookmarks from the SonicWALL SSL VPN Virtual Office home page.

Step 1 Type a descriptive name for the bookmark in the **Bookmark Name** field.

Step 2 Enter the fully qualified domain name (FQDN) or the IPv4 or, on SonicWALL SSL-VPN models 2000 and higher, IPv6 address of a host machine on the LAN in the **Name or IP Address** field. In some environments you can enter the host name only, such as when creating a VNC bookmark in a Windows local network.

Note If a Port number is included with an IPv6 address in the **Name or IP Address** field, the IPv6 address must be enclosed in square brackets, for example: **[2008::1:2:3:4]:6818**.

Note IPv6 is not supported by ActiveX or File Shares.

Some services can run on non-standard ports, and some expect a path when connecting. Depending on the choice in the Service field, format the **Name or IP Address** field like one of the examples shown in Table 14.

Table 14 Bookmark Name or IP Address Formats by Service Type

Service Type	Format	Example for Name or IP Address Field
RDP - ActiveX	IP Address	10.20.30.4
RDP - Java	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
VNC	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (mapped to session)	10.20.30.4:5901 (mapped to session 1)
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
	Note: Do not use session or display number instead of port.	**Note**: Do not use 10.20.30.4:1 **Tip**: For a bookmark to a Linux server, see the Tip below this table.
FTP	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
Telnet	IP Address	10.20.30.4
	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
SSHv1	IP Address	10.20.30.4
SSHv2	IPv6 Address	2008::1:2:3:4
	IP:Port (non-standard)	10.20.30.4:6818 or [2008::1:2:3:4]:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	Host name	JBJONES-PC
HTTP	URL	www.sonicwall.com
HTTPS	IP Address of URL	204.212.170.11
	IPv6 Address	2008::1:2:3:4
	URL:Path or File	www.sonicwall.com/index.html
	IP:Path or File	204.212.170.11/folder/
	URL:Port	www.sonicwall.com:8080
	IP:Port	204.212.170.11:8080 or [2008::1:2:3:4]:8080
	URL:Port:Path or File	www.sonicwall.com:8080/folder/index.html
	IP:Port:Path or File	204.212.170.11:8080/index.html

Service Type	Format	Example for Name or IP Address Field
File Shares	Host\Folder\	server-3\sharedfolder\
	Host\File	server-3\inventory.xls
	FQDN\Folder	server-3.company.net\sharedfolder\
	FQDN\File	server-3company.net\inventory.xls
	IP\Folder\	10.20.30.4\sharedfolder\
	IP\File	10.20.30.4\status.doc
		Note: Use backslashes even on Linux or Mac computers; these use the Windows API for file sharing.
Citrix (Citrix Web Interface)	IP Address	172.55.44.3
	IPv6 Address	2008::1:2:3:4
	IP:Port	172.55.44.3:8080 or [2008::1:2:3:4]:8080
	IP:Path or File	172.55.44.3/folder/file.html
	IP:Port:Path or File	172.55.44.3:8080/report.pdf
	FQDN	www.citrixhost.company.net
	URL:Path or File	www.citrixhost.net/folder/
	URL:Port	www.citrixhost.company.com:8080
	URL:Port:Path or File	www.citrixhost.com:8080/folder/index.html
	Note: *Port* refers to the HTTP(S) port of Citrix Web Interface, not to the Citrix ICA client port.	

Tip When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

Step 3 Optionally, you can enter a friendly description to be displayed in the bookmark table by filling in the **Description** field.

Step 4 Set whether users are can edit or delete bookmarks from the Virtual Office portal by making a selection for **Allow user to edit/delete**. You can select to **Allow**, **Deny**, or to **Use the user policy** setting.

Step 5 For the specific service you select from the **Service** drop-down list, additional fields may appear. Fill in the information for the service you selected. Select one of the following service types from the Service drop-down list:

Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)

Note If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark.

  Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.
- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Optionally enter the local path for this application in the **Application and Path (optional)** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select the **Login as console/admin session** checkbox to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Select the **Enable wake-on-LAN** checkbox to enable waking up a computer over the network connection. Selecting this checkbox causes the following new fields to be displayed:
  - **MAC/Ethernet Address** – Enter one or more MAC addresses, separated by spaces, of target hosts to wake.
  - **Wait time for boot-up (seconds)** – Enter the number of seconds to wait for the target host to fully boot up before cancelling the WoL operation.
  - **Send WOL packet to host name or IP address** – To send the WoL packet to the hostname or IP of this bookmark, select the **Send WOL packet to host name or IP address** checkbox, which can be applied in tandem with a MAC address of another machine to wake.
- For **RDP - ActiveX** on Windows clients, expand **Show client redirect options** and select any of the redirect checkboxes **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, or **Redirect SmartCards** to redirect those devices on the local network for use in this bookmark session. You can hover your mouse pointer over these options to display tooltips that indicate requirements for certain actions.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.
- For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advance Windows options** and select the checkboxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

Select the checkboxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.
Remote Application monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.

- For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces. Note that the RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. The **Enable plugin DLLs** option is not available for RDP - Java. See "Enabling Plugin DLLs" section on page 221.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Virtual Network Computing (VNC)

- No additional fields

File Transfer Protocol (FTP)

- Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Telnet

- No additional fields

Secure Shell version 1 (SSHv1)

- No additional fields

Secure Shell version 2 (SSHv2)

- Optionally select the **Automatically accept host key** checkbox.
- If using an SSHv2 server without authentication, such as a SonicWALL firewall, you can select the **Bypass username** checkbox.

Web (HTTP)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Secure Web (HTTPS)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

File Shares (CIFS)

- To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** checkbox.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

  When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SonicWALL SSL-VPN is not a domain member and will not be able to connect to the DFS shares.

  DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

Citrix Portal (Citrix)

- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.
- Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client or XenApp plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this checkbox leverages this portability.

Step 6 Click **Add** to update the configuration. Once the configuration has been updated, the new user bookmark will be displayed in the **Edit User Settings** window

Enabling Plugin DLLs

The plugin DLLs feature is available for RDP (ActiveX or Java), and allows for the use of certain third party programs such as print drivers, on a remote machine. This feature requires RDP Client Control version 5 or higher.

Note The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. No action (or checkbox) is needed.

To enable plugin DLLs for the RDP ActiveX client:

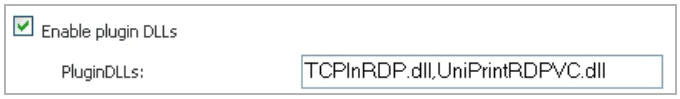
Step 1 Navigate to **Users > Local Users**.

Step 2 Click the configure icon corresponding to the user bookmark you wish to edit.

Step 3 In the **Bookmarks** tab, click **Add Bookmark**.

Step 4 Select **Terminal Services (RDP - ActiveX)** as the **Service** and configure as described in the section "Adding or Editing User Bookmarks" section on page 216.

Step 5 Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces.



Step 6 Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32).

Note Ensure that your Windows system and RDP client are up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

Creating a Citrix Bookmark for a Local User

Citrix support requires Internet connectivity in order to download the ActiveX or Java client from the Citrix Web site. Citrix is accessed from Internet Explorer using ActiveX by default, or from other browsers using Java. Java can be used with IE by selecting an option in the Bookmark configuration. The server will automatically decide which Citrix client version to use. For browsers requiring Java to run Citrix, you must have Sun Java 1.6.0_10 or above.

When using the Java applet, the local printers are available in the Citrix client. However, under some circumstances it might be necessary to change the Universal Printer Driver to PCL mode.

Note Citrix is supported on SonicWALL SSL-VPN model 2000 and higher security appliances.

To configure a Citrix bookmark for a user, perform the following tasks:

Step 1 Navigate to **Users > Local Users** and click the configure icon next to the user.

Step 2 In the **Edit User Settings** window, select the **Bookmarks** tab.

Step 3 Click **Add Bookmark...**

Step 4 Enter a name for the bookmark in the **Bookmark Name** field.

Step 5 Enter the name or IP address of the bookmark in the **Name or IP Address** field.

Note HTTPS, HTTP, Citrix, SSHv2, SSHv1, Telnet, and VNC will all take a port option *:portnum*. HTTP, HTTPS, and Fileshares can also have the path specified to a directory or file.

Step 6 From the **Service** drop-down list, select **Citrix Portal (Citrix)**. The display will change.

Step 7 Select the box next to **HTTPS Mode** to enable HTTPS mode.

Step 8 Optionally select the **Always use Java in Internet Explorer** checkbox to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client or XenApp plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this checkbox leverages this portability.

Step 9 Click **Add**.

Creating Bookmarks with Custom SSO Credentials

The administrator can configure custom Single Sign On (SSO) credentials for each user, group, or globally in HTTP(S), RDP (Java or ActiveX), File Shares (CIFS), and FTP bookmarks. This feature is used to access resources such as HTTP, RDP and FTP servers that need a domain prefix for SSO authentication. Users can log into SonicWALL SSL VPN as *username*, and click a customized bookmark to access a server with *domain\username*. Either straight textual parameters or dynamic variables may be used for login credentials.

To configure custom SSO credentials, and to configure Single Sign-On for Forms-based Authentication (FBA), perform the following steps:

Step 1 Create or edit a HTTP(S), RDP, File Shares (CIFS), or FTP bookmark as described in "Adding or Editing User Bookmarks" section on page 216.

Step 2 In the **Bookmarks** tab, select the **Use Custom Credentials** option

Step 3 Enter the appropriate username and password, or use dynamic variables as follows:

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%

Step 4 Enter the appropriate domain information in the **Domain** field.

Step 5 Select the Forms-based Authentication checkbox to configure Single Sign-On for Forms-based authentication.

- **User Form Field** - This should be the same as the 'name' and 'ID' attribute of the HTML element representing the User Name in the login form, for example:
  <input type=text name='userid'>

- **Password Form Field** - This should be the same as the ‘name’ or the ‘ID’ attribute of the HTML element representing Password in the login form, for example:
  <input type=password name=’PASSWORD’ id=’PASSWORD’ maxlength=128>

Step 6 Click **OK**.

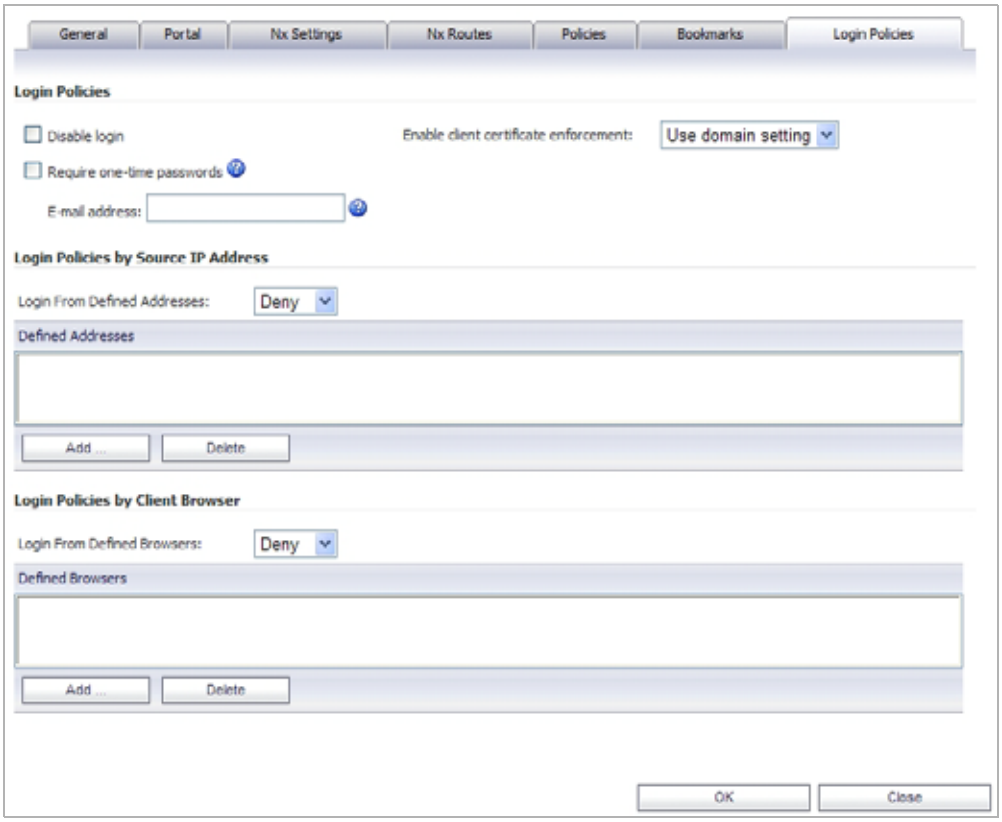
Configuring Login Policies

The **Login Policies** tab provides configuration options for policies that allow or deny users with specific IP addresses from having login privileges to the SonicWALL SSL-VPN appliance. To allow or deny specific users from logging into the appliance, perform the following steps:

Step 1 Navigate to the **Users > Local Users** page.

Step 2 Click the configure icon for the user you want to configure. The **Edit User Settings** dialog box is displayed.

Step 3 Click the **Login Policies** tab. The **Edit User Settings** - **Login Policies** tab is displayed.



Step 4 To block the specified user or users from logging into the appliance, select the **Disable login** checkbox.

Step 5 Optionally select the **Enable client certificate enforcement** checkbox to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this checkbox to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

Step 6 To require the use of one-time passwords for the specified user to log into the appliance, select the **Require one-time passwords** checkbox.

Step 7 Enter the user's email address into the **E-mail address** field to override any address provided by the domain. For more information about one-time passwords, see the "One Time Password Overview" section on page 28.

Note To configure email to external domains (for example, SMS addresses or external webmail addresses), you need to configure the SMTP server to allow relaying between the SSL-VPN and that domain.

Step 8 To apply the policy you selected to a source IP address, select an access policy (**Allow** or **Deny**) in the **Login From Defined Addresses** drop-down list under **Login Policies by Source IP Address**, and then click **Add** under the list box. The **Define Address** dialog box is displayed.

Step 9 In the **Define Address** dialog box, select one of the source address type options from the **Source Address Type** drop-down list.

- **IP Address** - Enables you to select a specific IP address.
- **IP Network** - Enables you to select a range of IP addresses. If you select this option, a **Network Address** field and **Subnet Mask** field appear in the **Define Address** dialog box.
- **IPv6 Address** - On SonicWALL SSL-VPN models 2000 and higher, this enables you to select a specific IPv6 address.
- **IPv6 Network** - On SonicWALL SSL-VPN models 2000 and higher, this enables you to select a range of IPv6 addresses. If you select this option, a **IPv6 Network** field and **Prefix** field appear in the **Define Address** dialog box.

Step 10 Provide appropriate IP address(es) for the source address type you selected.

- **IP Address** - Type a single IP address in the **IP Address** field.
- **IP Network** - Type an IP address in the **Network Address** field and then supply a subnet mask value that specifies a range of addresses in the **Subnet Mask** field.
- **IPv6 Address** - On SonicWALL SSL-VPN models 2000 and higher, type an IPv6 address, such as **2007::1:2:3:4**.
- **IPv6 Network** - On SonicWALL SSL-VPN models 2000 and higher, type the IPv6 network address into the **IPv6 Network** field, in the form **2007:1:2::**. Type a prefix into the **Prefix** field, such as **64**.

Step 11 Click **Add**. The address or address range is displayed in the **Defined Addresses** list in the **Edit User Settings** dialog box. As an example, if you selected a range of addresses with 10.202.4.32 as the network address and 255.255.255.240 (28 bits) as the subnet mask value,

the Defined Addresses list displays 10.202.4.32–10.202.4.47. In this case, 10.202.4.47 would be the broadcast address. Whatever login policy you selected will now be applied to addresses in this range.

Step 12 To apply the policy you selected to a client browser, select an access policy (**Allow** or **Deny**) in the **Login From Defined Browsers** drop-down list under **Login Policies by Client Browser**, and then click **Add** under the list. The **Define Browser** dialog box is displayed.

Step 13 In the **Define Browser** dialog box, type a browser definition in the **Client Browser** field and then click **Add**. The browser name appears in the Defined Browsers list.

Note The browser definition for Internet Explorer, Firefox, and Chrome is:
javascript:document:writeln(navigator.userAgent)

Step 14 Click **OK**. The new login policy is saved.

Users > Local Groups

This section provides an overview of the **Users > Local Groups** page and a description of the configuration tasks available on this page.

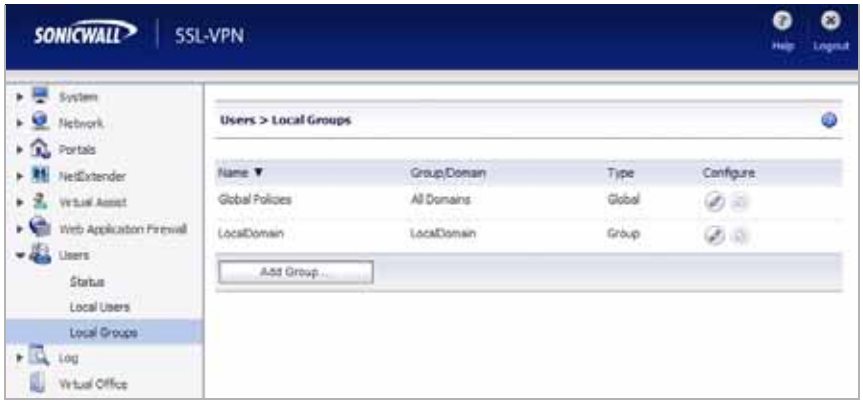
For a description of global settings for local groups, see the "Global Configuration" section on page 246.

Users > Local Groups Overview

The **Users > Local Groups** page allows the administrator to add and configure groups for granular control of user access by specifying a group name and domain.

Note that a group is automatically created when you create a domain. You can create domains in the **Portals > Domains** page. You can also create a group directly from the **Users** > **Local Groups** page.

Figure 28 Users > Local Groups Page



Adding a New Group

Note that a group is automatically created when you create a domain. You can create domains in the **Portals > Domains** page. You can also create a group directly from the **Users** > **Local Groups** page.

The **Users** > **Local Groups** window contains two default objects:

- **Global Policies** - Contains access policies for all nodes in the organization.
- **LocalDomain** - The LocalDomain group is automatically created to correspond to the default LocalDomain authentication domain. This is the default group to which local users will be added, unless otherwise specified.

To create a new group, perform the following steps:

Step 1 Click **Add Group**. The **Add Local Group** dialog box is displayed.

Step 2 In the **Add Local Group** dialog box, enter a descriptive name for the group in the **Group Name** field.

Step 3 Select the appropriate domain from the **Domain** drop-down list. The domain is mapped to the group.

Step 4 Click **Add** to update the configuration. Once the group has been added, the new group will be added to the **Local Groups** window.

All of the configured groups are displayed in the **Users > Local Groups** page, listed in alphabetical order.

Deleting a Group

To delete a group, click the delete icon in the row for the group that you wish to remove in the Local Groups table on the **Users > Local Groups** page. The deleted group will no longer appear in the list of defined groups.

Note A group cannot be deleted if users have been added to the group or if the group is the default group created for an authentication domain. To delete a group that is the default group for an authentication domain, delete the corresponding domain (you cannot delete the group in the **Edit Group Settings** window). If the group is not the default group for an authentication domain, first delete all users in the group. Then you will be able to delete the group on the **Edit Group Settings** page.

Editing Group Settings

To edit the settings for a group, click the configure icon in the row for the group that you wish to edit in the Local Groups table on the **Users > Local Groups** page. The Edit Group Settings window contains six tabs: **General**, **Portal**, **NxSettings**, **NxRoutes**, **Policies**, and **Bookmarks**.

See the following sections for information about configuring settings on these tabs:

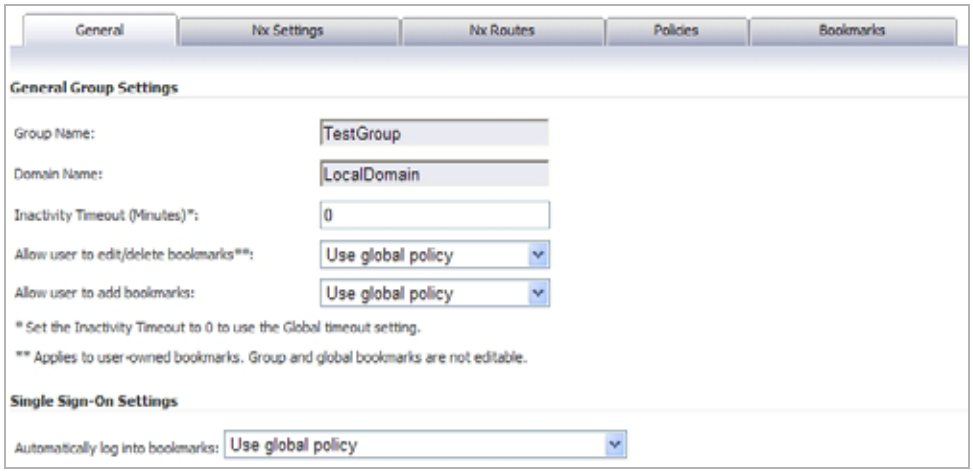
- “Editing General Group Settings” section on page 228
- “Modifying Group Portal Settings” section on page 230
- “Enabling Group NetExtender Settings” section on page 231
- “Enabling NetExtender Routes for Groups” section on page 232
- “Adding Group Policies” section on page 233
- “Editing a Policy for a File Share” section on page 235
- “Configuring Group Bookmarks” section on page 235

Editing General Group Settings

The **General** tab provides configuration options for a group’s inactivity timeout value and bookmark control. To modify the general user settings, perform the following tasks:

Step 1 In the left-hand column, navigate to the **Users** > **Local Groups**.

Step 2 Click the configure icon next to the group you want to configure. The **General** tab of the **Edit Group Settings** window displays. The **General** tab displays the following non-configurable fields: **Group Name** and **Domain Name**.



Step 3 To set the inactivity timeout for the group, meaning that users will be signed out of the Virtual Office after the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field.

Note The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

Step 4 To allow users to edit or delete user-owned bookmarks, select **Allow** from the **Allow user to edit/delete bookmarks** drop-down menu. To prevent users from editing or deleting user-owned bookmarks, select **Deny**. To use the group policy, select **Use group policy**.

Note Users cannot edit or delete group and global bookmarks.

Step 5 To allow users to add new bookmarks, select **Allow** from the **Allow user to add bookmarks** drop-down menu. To prevent users from adding new bookmarks, select **Deny**. To use the group policy, select **Use group policy**.

Step 6 Under Single Sign-On Settings, select one of the following options from the **Use SSL VPN account credentials to log into bookmarks** drop-down menu:

- **Use Global Policy**: Select this option to use the global policy settings to control single sign-on (SSO) for bookmarks.
- **User-controlled** (enabled by default for new users): Select this option to allow users to enable or disable single sign-on (SSO) for bookmarks. This setting enables SSO by default for new users.

Note Single sign-on (SSO) in SonicWALL SSL VPN does not support two-factor authentication.

- **User-controlled (disabled by default for new users)**: Select this option to allow users to enable or disable single sign-on (SSO) for bookmarks. This setting disables SSO by default for new users.
- **Enabled**: Select this option to enable single sign-on for bookmarks.
- **Disabled**: Select this option to disable single sign-on for bookmarks.

Step 7 Click **OK** to save the configuration changes.

Modifying Group Portal Settings

The **Portal** tab provides configuration options for portal settings for this group.

To configure portal settings for this group, perform the following steps:

Step 1 On the **Portal** tab under **Portal Settings**, for **NetExtender**, **Launch NetExtender after login**, **FileShares**, and **VirtualAssist**, select one of the following portal settings for this group:

- **Use portal setting** – The setting defined in the main portal settings will be used to determine if the portal feature is enabled or disabled. The main portal settings are defined by configuring the portal in the **Portals > Portals** page, on the **Home** tab of the Edit Portal screen.
- **Enabled** – Enable this portal feature for this user.
- **Disabled** – Disable this portal feature for this user.

Step 2 For **Allow User to Add Bookmarks** and **Allow User to Edit/Delete Bookmarks** select one of the following portal settings for this group:

- **Use global setting** – The setting defined globally will be used to determine if the portal feature is enabled or disabled. See “Edit Global Settings” section on page 246 for information about global settings.
- **Enabled** – Enable this portal feature for this user.
- **Disabled** – Disable this portal feature for this user.

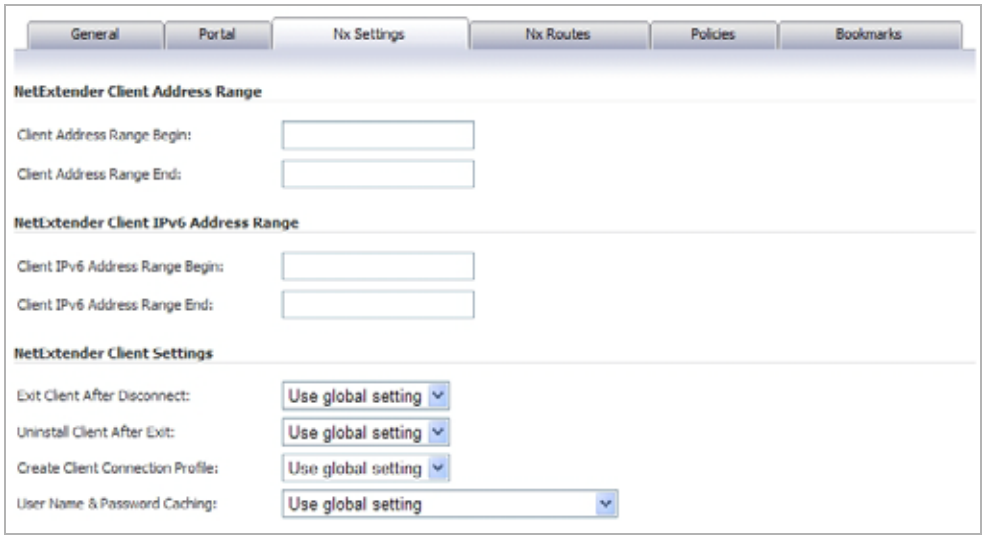
Note The **Allow User to Edit/Delete Bookmarks** setting applies to user-owned bookmarks only.

Step 3 Click **OK**.

Enabling Group NetExtender Settings

Note Group NetExtender settings are not supported on the SonicWALL SSL-VPN 200 appliance.

This feature is for external users, who will inherit the settings from their assigned group upon login. NetExtender client settings can be specified for the group, or use the global settings. For information about configuring global settings, see "Edit Global Settings" section on page 246.



To enable NetExtender ranges and configure client settings for a group, perform the following steps:

Step 1 Navigate to **Users > Local Groups.**

Step 2 Click the configure icon next to the group you want to configure.

Step 3 In the **Edit Group Settings** page, select the **NxSettings** tab.

Step 4 Enter a beginning IPv4 address in the **Client Address Range Begin** field.

Step 5 Enter an ending IPv4 address in the **Client Address Range End** field.

Step 6 On SonicWALL SSL-VPN models 2000 and higher, enter a beginning IPv6 address in the **Client IPv6 Address Range Begin** field.

Step 7 On SonicWALL SSL-VPN models 2000 and higher, enter an ending IPv6 address in the **Client IPv6 Address Range End** field.

Step 8 In the **Exit Client After Disconnect** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See "Edit Global Settings" section on page 246.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

Step 9 In the **Uninstall Client After Exit** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See "Edit Global Settings" section on page 246.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.

- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

Step 10 In the **Create Client Connection Profile** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See "Edit Global Settings" section on page 246.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

Step 11 In the **User Name & Password Caching** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See "Edit Global Settings" section on page 246.
- **Allow saving of user name only** - Allow caching of the user name for members of the group. Group members will only need to enter their password when starting NetExtender. Overrides the global setting.
- **Allow saving of user name & password** - Allow caching of the user name and password for members of the group. Group members will be automatically logged in when starting NetExtender. Overrides the global setting.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password for members of the group. Group members will be required to enter both user name and password when starting NetExtender. Overrides the global setting.

Step 12 Click **OK**.

Enabling NetExtender Routes for Groups

Note Group NetExtender routes are not supported on the SonicWALL SSL-VPN 200 appliance.

The **Nx Routes** tab allows the administrator to add and configure client routes. IPv6 client routes are supported on SonicWALL SSL-VPN model 2000 and higher appliances.

To enable multiple NetExtender routes for a group, perform the following steps:

Step 1 Navigate to **Users > Local Groups.**

Step 2 Click the configure icon next to the group you want to configure.

Step 3 In the **Edit Group Settings** page, select the **Nx Routes** tab.

Step 4 In the **Tunnel All Mode** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See "Edit Global Settings" section on page 246.
- **Enabled** - Force all traffic for this user, including traffic destined to the remote users' local network, over the SSL VPN NetExtender tunnel. Affects all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

Step 5 To add globally defined NetExtender client routes for members of this group, select the **Add Global NetExtender Client Routes** checkbox.

Step 6 Click **Add Client Route**.

Step 7 In the **Add Client Route** dialog box, enter a destination network in the **Destination Network** field. For example, enter the IPv4 network address 10.202.0.0. For IPv6, enter the IPv6 network address in the form 2007::1:2:3:0.

IPv6 is supported on SonicWALL SSL-VPN models 2000 and higher.

Step 8 For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

Step 9 Click **Add**.

Step 10 Click **OK**.

Enabling Group NetExtender Client Routes

To enable group NetExtender client routes for groups that are already created, perform the following steps:

Step 1 Navigate to **Users > Local Groups.**

Step 2 Click the configure icon next to the group you want to configure.

Step 3 In the **Edit Group Settings** page, select the **Nx Routes** tab.

Step 4 Select the **Add Global NetExtender Client Routes** checkbox.

Step 5 Click **OK**.

Enabling Tunnel All Mode for Local Groups

This feature is for external users, who will inherit the settings from their assigned group upon login. Tunnel all mode ensures that all network communications are tunneled securely through the SonicWALL SSL VPN tunnel. To enable tunnel all mode, perform the following tasks:

Step 1 Navigate to **Users > Local Groups.**

Step 2 Click the configure icon next to the group you want to configure.

Step 3 In the **Edit Group Settings** page, select the **Nx Routes** tab.

Step 4 Select **Enable** from the **Tunnel All Mode** drop-down list.

Step 5 Click **OK**.

Note You can optionally tunnel-all SSL VPN client traffic through the NetExtender connection by entering 0.0.0.0 for the Destination Network and Subnet Mask/Prefix in the Add Client Routes dialog box.

Adding Group Policies

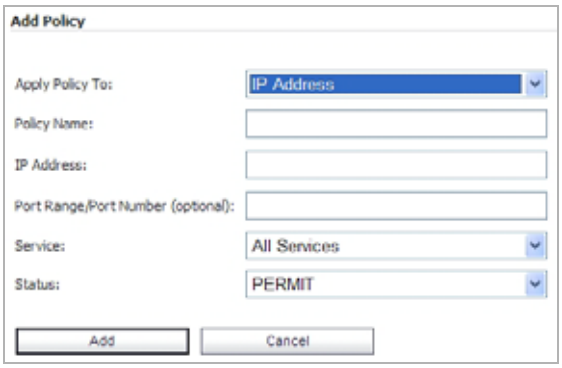
With group access policies, all traffic is allowed by default. Additional allow and deny policies may be created by destination address or address range and by service type.

The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.

Note User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address.

To define group access policies, perform the following steps:

Step 1 In the **Policies** tab, click **Add Policy**. The **Add Policy** window will be displayed.



Step 2 Define a name for the policy in the **Policy Name** field.

Step 3 In the **Apply Policy To** drop-down list, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. On SonicWALL SSL-VPN models 2000 and higher, you can also select an individual IPv6 host, a range of IPv6 addresses, or all IPv6 addresses. The **Add Policy** dialog box changes depending on what type of object you select in the **Apply Policy To** drop-down list.

Note The SonicWALL SSL VPN policies apply to the destination address(es) of the SonicWALL SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SonicWALL SSL VPN gateway through the policy engine. It is also possible to control source logins by IP address from the user's **Login Policies** page. For more information, refer to "Configuring Login Policies" section on page 224.

- **IP Address** - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field. Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.
- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally enter a port range (4100-4200) or a single port number into the **Port Range/Port Number** field.
- **Network Object -** If your policy applies to a predefined network object, select the name of the object from the **Network Object** drop-down list. A port or port range can be specified when defining a Network Object. See "Configuring Network Objects" section on page 101.
- **Server Path** - If your policy applies to a server path, select one of the following radio buttons in the R**esource** field:
  - **Share (Server path)** - When you select this option, type the path into the **Server Path** field.
  - **Network (Domain list)**
  - **Servers (Computer list)**

  See "Editing a Policy for a File Share" section on page 235.

- **URL Object** - If your policy applies to a predefined URL object, type the URL into the **URL** field.
- **IPv6 Address** - If your policy applies to a specific host, enter the IPv6 address of the local host machine in the **IPv6 Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field.

  IPv6 is supported on SonicWALL SSL-VPN models 2000 and higher.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information.

Step 4 Select the service type in the **Service** menu. If you are applying a policy to a network object, the service type is defined in the network object.

Step 5 Select **PERMIT** or **DENY** from the **Status** drop-down list to either permit or deny SonicWALL SSL VPN connections for the specified service and host machine.

Step 6 Click **Add** to update the configuration. Once the configuration has been updated, the new group policy will be displayed in the **Edit Group Settings** window. The group policies are displayed in the Group Policies list in the order of priority, from the highest priority policy to the lowest priority policy.

Editing a Policy for a File Share

To edit file share access policies, perform the following steps:

Step 1 Navigate to **Users > Local Groups**.

Step 2 Click the configure icon next to the group you want to configure.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy...**

Step 5 Select **Server Path** from the **Apply Policy To** drop-down list.

Step 6 Type a name for the policy in the **Policy Name** field.

Step 7 In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername**share**path*. The prefixes \\, //, \ and / are acceptable.

Note Share and path provide more granular control over a policy. Both are optional.

Step 8 Select **PERMIT** or **DENY** from the **Status** drop-down list.

Step 9 Click **Add**.

Configuring Group Bookmarks

SonicWALL SSL VPN bookmarks provide a convenient way for SonicWALL SSL VPN users to access computers on the local area network that they will connect to frequently. Group bookmarks will apply to all members of a specific group. To define group bookmarks, perform the following steps:

Step 1 Navigate to the **Users** > **Local Groups** window.

Step 2 Click the configure icon for the group for which you want to create a bookmark. The **Edit Group Settings** dialog box is displayed.

Step 3 Navigate to the **Bookmarks** tab and click **Add Bookmark**. The **Add Bookmark** window is displayed.

Note When group bookmarks are defined, all group members will see the defined bookmarks from the SonicWALL SSL VPN user portal. Individual group members will not be able to delete or modify group bookmarks.

Step 4 Enter a string that will be the name of the bookmark in the **Bookmark Name** field.

Enter the fully qualified domain name (FQDN) or the IPv4 or, on SonicWALL SSL-VPN models 2000 and higher, IPv6 address of a host machine on the LAN in the **Name or IP Address** field. In some environments you can enter the host name only, such as when creating a VNC bootmark in a Windows local network.

Note If a Port number is included with an IPv6 address in the **Name or IP Address** field, the IPv6 address must be enclosed in square brackets, for example: **[2008::1:2:3:4]:6818**. IPv6 is not supported for RDP - ActiveX, RDP - Java, File Shares, or VNC bookmarks.

Note For HTTP and HTTPS, you can add a custom port and path, for example, servername:port/path. For VNC, Telnet, and SSH, you can add a custom port, for example, servername:port.

Step 5 For the specific service you select from the **Service** drop-down list, additional fields may appear. Fill in the information for the service you selected.

Note Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

Select one of the following service types from the **Service** drop-down list:

Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)

Note If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

- In the **Screen Size** drop-down menu, select the default terminal services screen size to be used when users execute this bookmark.
- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Optionally enter the local path for this application in the **Application and Path (optional)** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.

– Select the **Login as console/admin session** checkbox to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.

– Select the **Enable wake-on-LAN** checkbox to enable waking up a computer over the network connection. Selecting this checkbox causes the following new fields to be displayed:

  • **MAC/Ethernet Address** – Enter one or more MAC addresses, separated by spaces, of target hosts to wake.

  • **Wait time for boot-up (seconds)** – Enter the number of seconds to wait for the target host to fully boot up before cancelling the WoL operation.

  • **Send WOL packet to host name or IP address** – To send the WoL packet to the hostname or IP of this bookmark, select the **Send WOL packet to host name or IP address** checkbox, which can be applied in tandem with a MAC address of another machine to wake.

– For **RDP - ActiveX** on Windows clients, expand **Show client redirect options** and select any of the redirect checkboxes **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, or **Redirect SmartCards** to redirect those devices on the local network for use in this bookmark session. You can hover your mouse pointer over these options to display tooltips that indicate requirements for certain actions.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

– For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advanced Windows options** and select the checkboxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

  Select the checkboxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

  If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.
  Remote Application monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.

– For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces. Note that the RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. This option is not available for RDP - Java.

– Select the **Enable wake on LAN** checkbox to send WoL packets to the host. Selecting this option displays additional fields for entering one or more **Mac Address**es (separated by spaces) to indicate 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** checkbox, which can be applied in tandem with a Mac address of another machine to wake.

– Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Virtual Network Computing (VNC)

– No additional fields

File Transfer Protocol (FTP)

– Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.

– Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Telnet

– No additional fields

Secure Shell version 1 (SSHv1)

– No additional fields

Secure Shell version 2 (SSHv2)

– Optionally select the **Automatically accept host key** checkbox.

– If using an SSHv2 server without authentication, such as a SonicWALL firewall, you can select the **Bypass username** checkbox.

Web (HTTP)

– Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Secure Web (HTTPS)

– Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

File Shares (CIFS)

– To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** checkbox.

– Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see "Creating Bookmarks with Custom SSO Credentials" section on page 223.

Citrix Portal (Citrix)

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

– Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client or XenApp plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this checkbox leverages this portability.

Step 6 Click **Add** to update the configuration. Once the configuration has been updated, the new group bookmark will display in the **Edit Group Settings** window.

Group Configuration for LDAP Authentication Domains

Note The Microsoft Active Directory database uses an LDAP organization schema. The Active Directory database may be queried using Kerberos authentication (the standard authentication type; this is labeled "Active Directory" domain authentication in the SonicWALL SSL VPN management interface), NTLM authentication (labeled NT Domain authentication in SonicWALL SSL VPN management interface), or using LDAP database queries. An LDAP domain configured in the SonicWALL SSL VPN management interface can authenticate to an Active Directory server.

LDAP (Lightweight Directory Access Protocol) is a standard for querying and updating a directory. Since LDAP supports a multilevel hierarchy (for example, groups or organizational units), the SonicWALL SSL-VPN appliance can query this information and provide specific group policies or bookmarks based on LDAP attributes. By configuring LDAP attributes, the SonicWALL SSL-VPN appliance administrator can leverage the groups that have already been configured in an LDAP or Active Directory database, rather than needing to manually recreate the same groups in the SonicWALL SSL-VPN appliance.

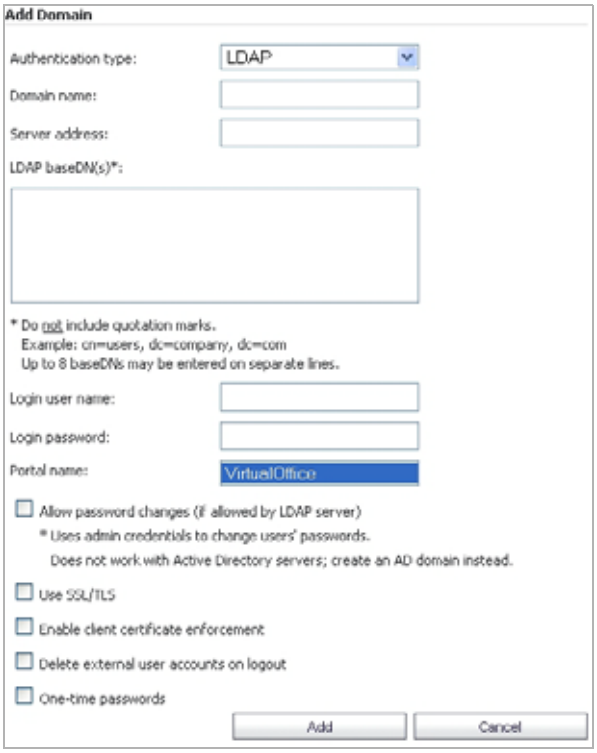
Once an LDAP authentication domain is created, a default LDAP group will be created with the same name as the LDAP domain name. Although additional groups may be added or deleted from this domain, the default LDAP group may not be deleted. If the user for which you created LDAP attributes enters the Virtual Office home page, the bookmark you created for the group the user is in will display in the Bookmarks Table.

For an LDAP group, you may define LDAP attributes. For example, you can specify that users in an LDAP group must be members of a certain group or organizational unit defined on the LDAP server. Or you can specify a unique LDAP distinguished name.

To add an LDAP attribute for a group so that a user will have a bookmark assigned when entering the Virtual Office environment, perform the following steps:

Step 1 Navigate to the **Portals > Domains** page and click **Add Domain** to display the **Add New Domain** dialog box.

Step 2 Select LDAP from the **Authentication Type** menu. The LDAP domain configuration fields will be displayed.



Step 3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL VPN user portal. It can be the same value as the **Server address** field.

Step 4 Enter the IP address or domain name of the server in the **Server address** field.

Step 5 Enter the search base for LDAP queries in the **LDAP baseDN** field. An example of a search base string is **CN=Users,DC=yourdomain,DC=com**.

Tip It is possible for multiple OUs to be configured for a single domain by entering each OU on a separate line in the **LDAP baseDN** field. In addition, any sub-OUs will be automatically included when parents are added to this field.

Note Do not include quotes (“”) in the **LDAP BaseDN** field.

Step 6 Enter the common name of a user that has been delegated control of the container that user will be in along with the corresponding password in the **Login user name** and **Login password** fields.

Note When entering **Login user name** and **Login password**, remember that the SSL-VPN appliance binds to the LDAP tree with these credentials and users can log in with their sAMAccountName.

Step 7 Enter the name of the portal in the **Portal name** field. Additional layouts may be defined in the **Portals > Portals** page.

Step 8 Select the **Allow password changes (if allowed by LDAP server)** checkbox if you want to be able to change user's passwords. The admin account must be used when changing user passwords.

Step 9 Select the **Delete external user accounts on logout** checkbox to delete users who are not logged into a domain account after they log out.

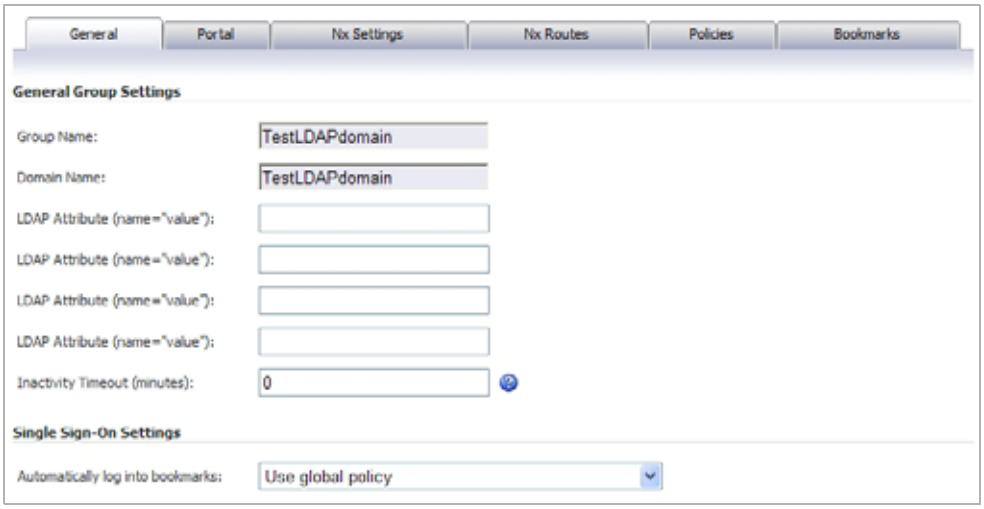
Step 10 Optionally select the **One-time passwords** checkbox to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

Step 11 If you select **One-time passwords**, an **LDAP e-mail attribute** drop-down list appears. Select one of the following:

- **mail** - Select **mail** if this is the name of your LDAP email attribute.
- **userPrincipalName** - Select **userPrincipalName** if this is the name of your LDAP email attribute.
- **custom** - Select **custom** to enter any other LDAP email attribute. Enter the attribute name into the **Custom attribute** field that appears.

Step 12 Navigate to the **Users > Local Groups** page and click the configure icon. The **Edit Group Settings** page is displayed, with fields for LDAP attributes on the **General** tab.



Step 13 On the **General** tab, you may optionally fill out one or multiple **LDAP Attribute** fields with the appropriate names where **name=value** is the convention for adding a series of LDAP attributes. To see a full list of LDAP attributes, refer to the SonicWALL LDAP Attribute document.

As a common example, fill out an attribute field with the memberOf= attribute which can bundle the following common variable types:

CN= - the common name. DN= - the distinguished name. DC= - the domain component.

You need to provide quote delimiters around the variables you bundle in the memberOf line. You separate the variables by commas. An example of the syntax using the **CN** and **DC** variables would be:

memberOf="CN=<string>, DC=<string>

An example of a line you might enter into the **LDAP Attribute** field, using the **CN** and **DC** variables would be:

memberOf="CN=Terminal Server Computers,CN=Users,DC=sonicwall,DC=net"

Step 14 Type an inactivity timeout value (in minutes) in the **Inactivity Timeout** field. Enter **0** (zero) to use the global inactivity timeout setting.

Step 15 Under **Single Sign-On Settings**, in the **Automatically log into bookmarks list**, select one of the following:

- **Use global policy** – Use the global policy for using SSO to login to bookmarks.
- **User-controlled (enabled by default for new users)** – Enable SSO to login to bookmarks for new users, and allow users to change this setting.
- **User-controlled (disabled by default for new users)** – Disable SSO to login to bookmarks for new users, and allow users to change this setting.
- **Enabled** – Enable SSO to login to bookmarks
- **Disabled** – Disable SSO to login to bookmarks

Step 16 Click **OK** when done.

LDAP Attribute Information

When configuring LDAP attributes, the following information may be helpful:

- If multiple attributes are defined for a group, all attributes must be met by LDAP users.
- LDAP authentication binds to the LDAP tree using the same credentials as are supplied for authentication. When used against Active Directory, this requires that the login credentials provided match the CN (common name) attribute of the user rather than samAccountName (login name). For example, if your NT/Active Directory login name is **gkam** and your full name is **guitar kam,** when logging into SonicWALL SSL VPN with LDAP authentication, the username should be provided in the following ways: If a login name is supplied, that name is used to bind to the tree. If the field is blank, you need to login with the full name. If the field is filled in with a full login name, users will login with the sAMAccountName.
- If no attributes are defined, then any user authorized by the LDAP server can be a member of the group.
- If multiple groups are defined and a user meets all the LDAP attributes for two groups, then the user will be considered part of the group with the most LDAP attributes defined. If the matching LDAP groups have an equal number of attributes, then the user will be considered a member of the group based on the alphabetical order of the groups.
- If an LDAP user fails to meet the LDAP attributes for all LDAP groups configured on the SonicWALL SSL-VPN appliance, then the user will not be able to log into the portal. So the LDAP attributes feature not only allows the administrator to create individual rules based on the LDAP group or organization, it also allows the administrator to only allow certain LDAP users to log into the portal.

Example of LDAP Users and Attributes

If a user is manually added to a LDAP group, then the user setting will take precedence over LDAP attributes.

For example, an LDAP attribute **objectClass="Person"** is defined for group Group1 and an LDAP attribute **memberOf="CN=WINS Users,DC=sonicwall,DC=net** is defined for Group2.

If user Jane is defined by an LDAP server as a member of the Person object class, but is not a member of the WINS Users group, Jane will be a member of SonicWALL SSL-VPN appliance Group1.

But if the administrator manually adds the user Jane to SonicWALL SSL-VPN appliance Group2, then the LDAP attributes will be ignored and Jane will be a member of Group2.

Sample LDAP Attributes

You may enter up to four LDAP attributes per group. The following are some example LDAP attributes of Active Directory LDAP users:

```
name="Administrator"
memberOf="CN=Terminal Server Computers,CN=Users,DC=sonicwall,DC=net"
objectClass="user"
msNPAllowDialin="FALSE"
```

Querying an LDAP Server

If you would like to query your LDAP or Active Directory server to find out the LDAP attributes of your users, there are several different methods. From a machine with ldapsearch tools (for example a Linux machine with OpenLDAP installed) run the following command:

```
ldapsearch -h 10.0.0.5 -x -D
"cn=demo,cn=users,dc=sonicwall,dc=net" -w demo123 –b
"dc=sonicwall,dc=net" > /tmp/file
```

Where:

- **10.0.0.5** is the IP address of the LDAP or Active Directory server
- **cn=demo,cn=users,dc=sonicwall,dc=net** is the distinguished name of an LDAP user
- **demo123** is the password for the user demo
- **dc=sonicwall,dc=net** is the base domain that you are querying
- **> /tmp/file** is optional and defines the file where the LDAP query results will be saved.

For instructions on querying an LDAP server from a Window server, refer to:

- www.microsoft.com/Resources/Documentation/ windowsserv/2003/all/techref/en-us/w2k3tr_adsrh_what.asp
- http://www.microsoft.com/Resources/Documentation/windowsserv/2003/all/techref/en-us/w2k3tr_adsrh_how.asp?frame=true

Group Configuration for Active Directory, NT and RADIUS Domains

For authentication to RADIUS, Microsoft NT domain or Active Directory servers (using Kerberos), you can individually define AAA users and groups. This is not required, but it enables you to create separate policies or bookmarks for individual AAA users.

When a user logs in, the SonicWALL SSL-VPN appliance will validate with the appropriate Active Directory, RADIUS, or NT server that the user is authorized to login. If the user is authorized, the SonicWALL SSL-VPN appliance will check to see if a user exists in the SonicWALL SSL-VPN appliance database for users and groups. If the user is defined, then the policies and bookmarks defined for the user will apply.

For example, if you create a RADIUS domain in the SonicWALL SSL-VPN appliance called “Miami RADIUS server”, you can add users to groups that are members of the “Miami RADIUS server” domain. These user names must match the names configured in the RADIUS server. Then, when users login to the portal, policies, bookmarks and other user settings will apply to the users. If the AAA user does not exist in the SonicWALL SSL-VPN appliance, then only the global settings, policies and bookmarks will apply to the user.

This section contains the following subsections:

- “Bookmark Support for External (Non-Local) Users” section on page 244
- “Adding a RADIUS Group” section on page 244
- “Adding an Active Directory Group” section on page 245

Bookmark Support for External (Non-Local) Users

The Virtual Office bookmark system allows bookmarks to be created at both the group and user levels. The administrator can create both group and user bookmarks which will be propagated to applicable users, while individual users can create only personal bookmarks.

Since bookmarks are stored within the SonicWALL SSL-VPN'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 (LocalDomain) groups and users, this is automated since the administrator must manually define the groups and users on the appliance. Similarly, when working with external (non-LocalDomain, for example, RADIUS, NT, LDAP) groups, the correlation is automated since creating an external domain creates a corresponding local group.

However, when working with external (non-LocalDomain) users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SonicWALL SSL-VPN's configuration files. The need to store bookmarks on the SonicWALL SSL-VPN 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 to use personal bookmarks, SonicWALL SSL VPN automatically creates a corresponding local user entity upon user login. Bookmarks can be added to the locally-created user.

For example, if a RADIUS domain called myRADIUS is created, and RADIUS user jdoe logs on to the SonicWALL SSL-VPN, the moment jdoe adds a personal bookmark, a local user called jdoe will be created on the SonicWALL SSL-VPN appliance as type External, and can then be managed like any other local user by the administrator. The external local user will remain until deleted by the administrator.

Adding a RADIUS Group

Note Before configuring RADIUS groups, ensure that the RADIUS Filter-Id option is enabled for the RADIUS Domain to which your group is associated. This option is configured in the **Portals > Domains** page.

The **RADIUS Groups** tab allows the administrator to enable user access to the SSL-VPN based on existing RADIUS group memberships. By adding one or more RADIUS groups to an SSL VPN group, only users associated with specified RADIUS group(s) are allowed to login. To add a RADIUS group, perform the following steps:

Step 1 In the **Users > Local Groups** page, click the configure button for the RADIUS group you want to configure.

Step 2 In the **RADIUS Groups** tab and click the **Add Group...** button. The Add RADIUS Group page displays.

Step 3 Enter the **RADIUS Group** name in the corresponding field. The group name must match the RADIUS Filter-Id exactly.

Step 4 Click the **Add** button. The group displays in the RADIUS Groups section.

Adding an Active Directory Group

On SSL-VPN models 2000 and higher, the **AD Groups** tab allows the administrator to enable user access to the SSL-VPN based on existing AD group memberships. By adding one or more AD groups to an SSL VPN group, only users associated with specified AD group(s) are allowed to login.

Note Before configuring and Active Directory group, ensure that you have already created an Active Directory domain. This option is configured in the **Portals > Domains** page.

Note The AD Groups feature is only available on SonicWALL SSL-VPN models 2000 and higher.

To add an AD group, perform the following steps:

Step 1 In the **Users > Local Groups** page, click the configure button for the AD group you want to configure.

Step 2 In the **AD Groups** tab and click the **Add Group...** button. The Add Active Directory Group page displays.

Step 3 Enter the **Active Directory Group** name in the corresponding field.

Step 4 Click the **Add** button. The group displays in the Active Directory Groups section. The process of adding a group may take several moments. Do not click the Add button more than once during this process.

Creating a Citrix Bookmark for a Local Group

(Supported on Windows, MacOS, and Linux.) The Citrix support feature is supported on SonicWALL SSL-VPN model 2000 and higher security appliances. To configure a Citrix bookmark for a user, perform the following tasks:

Step 1 Navigate to **Users > Local Group**s.

Step 2 Click the configure icon next to the group you want to configure.

Step 3 In the **Edit Group Settings** window, select the **Bookmarks** tab.

Step 4 Click **Add Bookmark...**

Step 5 Enter a name for the bookmark in the **Bookmark Name** field.

Step 6 Enter the name or IP address of the bookmark in the **Name or IP Address** field.

Step 7 From the **Service** drop-down list, select **Citrix Portal (Citrix)**. A checkbox for **HTTPS Mode** displays.

Step 8 Optionally select the **HTTPS Mode** checkbox to enable HTTPS mode.

Step 9 Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE.

Step 10 Click **OK**.

Global Configuration

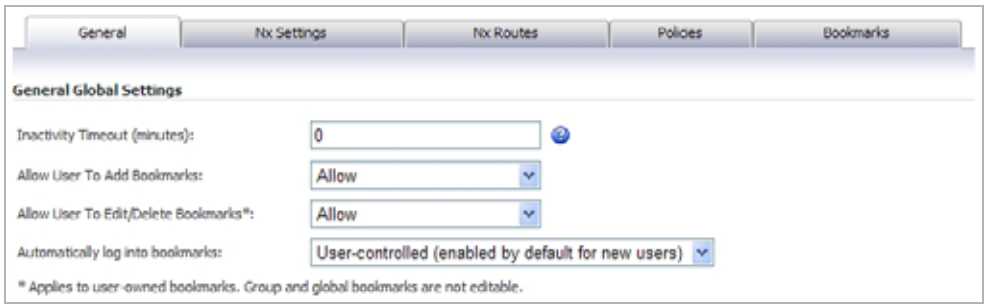
SonicWALL SSL-VPN appliance global configuration is defined from the **Local Users** or **Local Groups** environment. To view either, click the **Users** option in the left navigation menu, then click either the **Local Users** or **Local Groups** option. This section contains the following configuration tasks:

Edit Global Settings

To edit global settings, perform the following steps:

Step 1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

Step 2 Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.



Step 3 On the **General** tab, to set the inactivity timeout for all users or groups, meaning that users will be signed out of the Virtual Office after the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field.

Note The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

Step 4 To allow users to add new bookmarks, select **Allow** from the **Allow User to Add Bookmarks** drop-down menu. To prevent users from adding new bookmarks, select **Deny**.

Step 5 To allow users to edit or delete user-owned bookmarks, select **Allow** from the **Allow User to Edit/Delete Bookmarks** drop-down menu. To prevent users from editing or deleting user-owned bookmarks, select **Deny**.

Note Users cannot edit or delete group and global bookmarks.

Step 6 In the **Automatically log into bookmarks** drop-down list, select one of the following options:

- **User-controlled (enabled by default for new users)**: Select this option to allow users to enable or disable single sign-on (SSO) automatic login for bookmarks. This setting enables automatic login by default for new users.
- **User-controlled (disabled by default for new users)**: Select this option to allow users to enable or disable single sign-on (SSO) automatic login for bookmarks. This setting disables automatic login by default for new users.
- **Enabled**: Select this option to enable automatic login for bookmarks.
- **Disabled**: Select this option to disable automatic login for bookmarks.

Step 7 Click **OK** to save the configuration changes.

Step 8 Navigate to the **Nx Settings** tab.

Step 9 To set a client address range, enter a beginning address in the **Client Address Range Begin** field and an ending address in the **Client Address Range End** field.

Step 10 On SonicWALL SSL-VPN models 2000 and higher, to set a client IPv6 address range, enter a beginning IPv6 address in the **Client IPv6 Address Range Begin** field and an ending IPv6 address in the **Client IPv6 Address Range End** field.

Step 11 In the **Exit Client After Disconnect** drop-down list, select **Enabled** or **Disabled**.

Step 12 In the **Uninstall Client After Exit** drop-down list, select **Enabled** or **Disabled**.

Step 13 In the **Create Client Connection Profile** drop-down list, select **Enabled** or **Disabled**.

Step 14 In the **User Name & Password Caching** drop-down list, select one of the following:

- **Allow saving of user name only** - Allow caching of the user name on the client. Users will only need to enter their password when starting NetExtender.
- **Allow saving of user name & password** - Allow caching of the user name and password on the client. Users will be automatically logged in when starting NetExtender, after the first login.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password on the client. Users will be required to enter both user name and password when starting NetExtender.

Step 15 Navigate to the **Nx Routes** tab.

Step 16 In the **Tunnel All Mode** drop-down list, select **Enabled** to force all traffic for the user, including traffic destined to the remote user's local network, over the SSL VPN NetExtender tunnel. **Tunnel All Mode** is disabled by default.

Step 17 To add a client route, click **Add Client Route...**

Step 18 In the **Add Client Route** dialog box, enter a destination network in the **Destination Network** field. For example, enter the IPv4 network address 10.202.0.0. For IPv6, enter the IPv6 network address in the form 2007::1:2:3:0.

IPv6 is supported on SonicWALL SSL-VPN models 2000 and higher.

Step 19 For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

Step 20 Click **Add**.

Step 21 Click **OK** to save the configuration changes.

Step 22 Navigate to the **Policies** tab.

Step 23 To add a policy, click **Add Policy...**

Step 24 In the **Apply Policy To** drop-down list, select one of the following: **IP Address**, **IP Address Range**, **All Addresses**, **Network Object**, **Server Path**, **URL Object**, **All IPv6 Address**, **IPv6 Address**, or **IPv6 Address Range**.

Step 25 Enter a name for the policy in the **Policy Name** field.

Step 26 In the fields that appear based on your **Apply Policy To** settings, fill in the appropriate information. For example, if you select **IP Address** in the **Apply Policy To** drop-down list, you will need to supply the IP Address in the **IP Address** field and the service in the **Service** drop-down list. If you select **IPv6 Address Range**, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field. This field is available when you select **IP Address**, **IP Address Range**, **IPv6 Address**, or **IPv6 Address Range** in the **Apply Policy To** drop-down list.

Step 27 Click **Add**.

Step 28 Click **OK** to save the configuration changes.

Step 29 Click the **Bookmarks** tab.

Step 30 To add a bookmark, click **Add Bookmark...**

Step 31 Enter a bookmark name in the **Bookmark Name** field.

Step 32 Enter the bookmark name or IP address in the **Name or IP Address** field.

Step 33 Select one of the following services from the **Service** drop-down list: **Terminal Services (RDP - ActiveX)**, **Terminal Services (RDP - Java)**, **Virtual Network Computing (VNC)**, **Citrix Portal (Citrix)**, **Web (HTTP)**, **Secure Web (HTTPS)**, **File Shares (CIFS)**, **File Transfer Protocol (FTP)**, **Telnet, Secure Shell Version 1 (SSHv1)**, or **Secure Shell Version 2(SSHv2)**.

Note IPv6 is not supported on File Shares bookmarks.

Step 34 In the fields that appear based on your **Service** settings, fill in the appropriate information. For example, if you select **Terminal Services (RDP - ActiveX)**, you will need to select the desired screen size from the **Screen Size** drop-down list.

Step 35 Click **Add**.

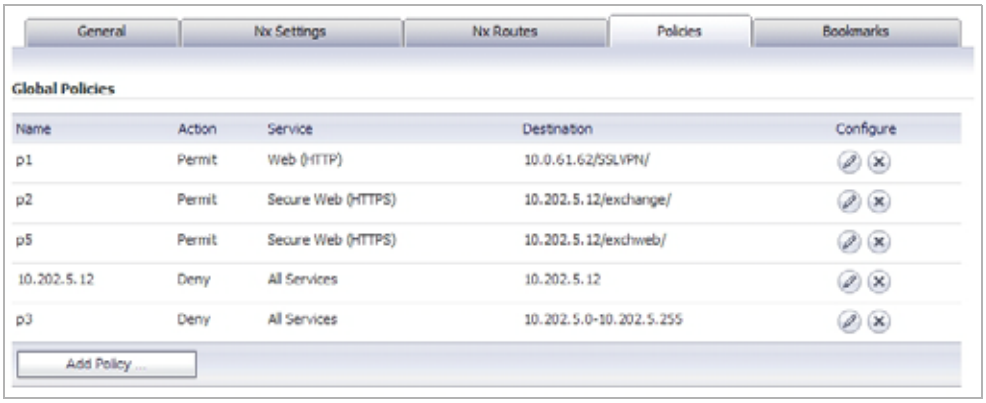
Step 36 Click **OK** to save the configuration changes.

Edit Global Policies

To define global access policies, perform the following steps:

Step 1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

Step 2 Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.



Step 3 On the **Policies** tab, click **Add Policy**. The **Add Policy** window is displayed.

Note User and group access policies will take precedence over global policies.

Step 4 In the **Apply Policy To** drop-down list, select one of the following: **IP Address**, **IP Address Range**, **All Addresses**, **Network Object**, **Server Path**, **URL Object**, **All IPv6 Address**, **IPv6 Address**, or **IPv6 Address Range**.

IPv6 is supported only on SonicWALL SSL-VPN models 2000 and higher.

Step 5 Type a name for the policy in the **Policy Name** field.

Note SonicWALL SSL-VPN appliance policies apply to the destination address(es) of the SonicWALL SSL VPN connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SonicWALL SSL-VPN appliance through the policy engine.

- If your policy applies to a specific IPv4 host, select the **IP Address** option from the **Apply Policy To** drop-down list and enter the IPv4 address of the local host machine in the **IP Address** field.
- If your policy applies to a range of IPv4 addresses, select the **IP Address Range** option from the **Apply Policy To** drop-down list and enter the IPv4 network address in the **IP Network Address** field and the subnet mask in the **Subnet Mask** field.
- If your policy applies to a specific IPv6 host, select the **IPv6 Address** option from the **Apply Policy To** drop-down list and enter the IPv6 address of the local host machine in the **IPv6 Address** field.
- If your policy applies to a range of IPv6 addresses, select the **IPv6 Address Range** option from the **Apply Policy To** drop-down list and enter the IPv6 network address in the **IPv6 Network Address** field and the IPv6 prefix in the **IPv6 Prefix** field.

Step 6 Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field. This field is available when you select **IP Address**, **IP Address Range**, **IPv6 Address**, or **IPv6 Address Range** in the **Apply Policy To** drop-down list.

Step 7 Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

Step 8 Select **ALLOW** or **DENY** from the **Status** drop-down list to either permit or deny SonicWALL SSL VPN connections for the specified service and host machine.

Step 9 Click **Add** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Edit Global Settings** window. The global policies will be displayed in the policy list in the **Edit Global Settings** window in the order of priority, from the highest priority policy to the lowest priority policy.

Edit a Policy for a File Share

To edit file share access policies, perform the following steps:

Step 1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

Step 2 Click the configure icon next to **Global Policies**. The **Edit Global Settings** window will be displayed.

Step 3 Select the **Policies** tab.

Step 4 Click **Add Policy**.

Step 5 Select **Server Path** from the **Apply Policy To** drop-down list.

Step 6 Type a name for the policy in the **Policy Name** field.

Step 7 In the **Resource** field, select one of the following radio buttons for the type of resource:

- **Share (Server path)**
- **Network (Domain list)**
- **Servers (Computer list)**

Step 8 In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername**share**path*. The prefixes \\, //, \ and / are acceptable.

Note Share and path provide more granular control over a policy. Both are optional.

Step 9 Select **PERMIT** or **DENY** from the **Status** drop-down list.

Step 10 Click **Add**.

Edit Global Bookmarks

To edit global bookmarks, perform the following steps:

Step 1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

Step 2 Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

Step 3 Click **Add Bookmark**. An **Add Bookmark** window will be displayed.

Note When global bookmarks are defined, all users will see the defined bookmarks from the SonicWALL SSL VPN user portal. Individual users will not be able to delete or modify global bookmarks.

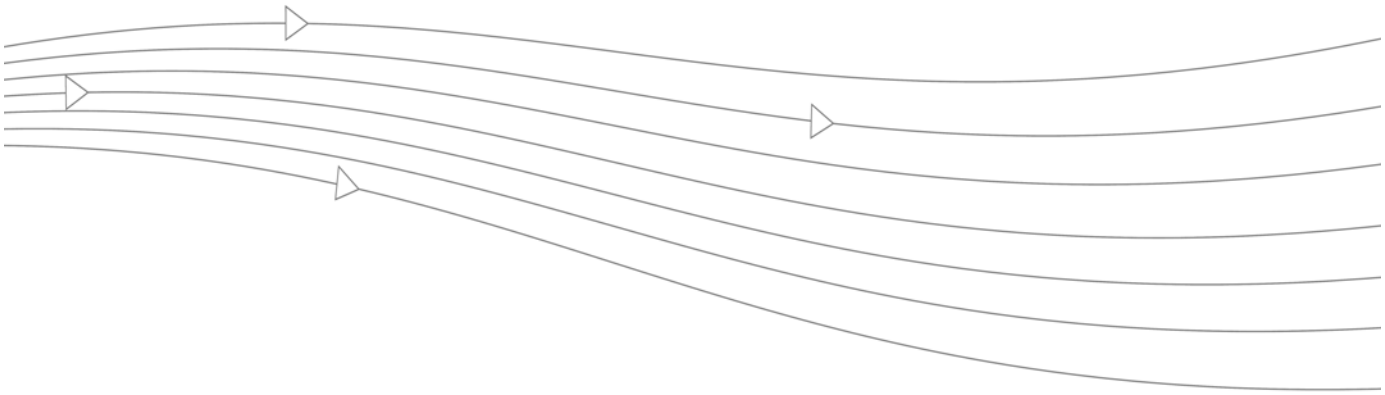
Step 4 To edit a bookmark, enter a descriptive name in the **Bookmark Name** field.

Step 5 Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.

Step 6 Select the service type in the **Service** drop-down list.

Note Depending on the service you select from the **Service** drop-down list, additional fields may appear. Fill in the information based on the service you select. For example, if you select **RDP - ActiveX** or **RDP - Java**, a **Screen Size** drop-down list and other additional fields are displayed.

Step 7 Click **Add** to update the configuration. Once the configuration has been updated, the new global bookmark will be displayed in the bookmarks list in the **Edit Global Settings** window.



Chapter 10: Log Configuration

This chapter provides information and configuration tasks specific to the **Log** pages on the SonicWALL SSL VPN Web-based management interface.

This chapter contains the following sections:

Log > View

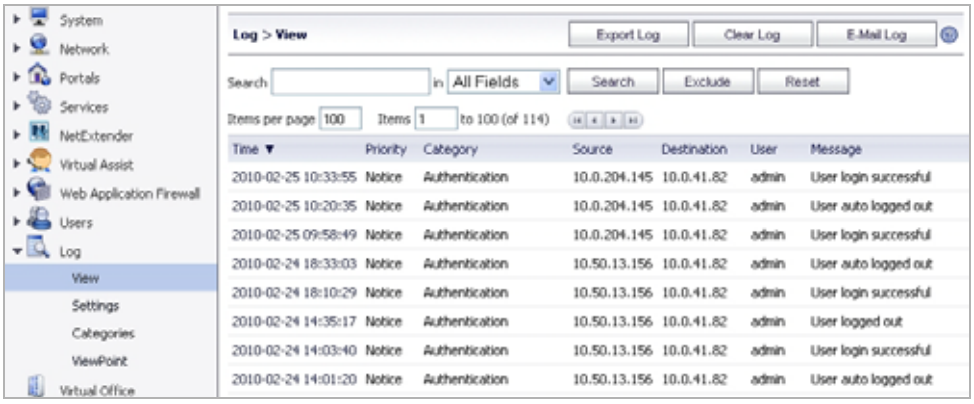
SonicWALL SSL VPN supports Web-based logging, syslog logging and email alert messages. In addition, SonicWALL SSL VPN may be configured to email the event log file to the SonicWALL SSL VPN administrator before the log file is cleared.

This section provides an overview of the **Log > View** page and a description of the configuration tasks available on this page.

Log > View Overview

The **Log > View** page allows the administrator to view the SonicWALL SSL VPN event log. The event log can also be automatically sent to an email address for convenience and archiving.

Figure 29 Log > View



The **Log > View** page displays log messages in a sortable, searchable table. The SonicWALL SSL-VPN appliance can store 250 Kilobytes of log data or approximately 1,000 log messages. Each log entry contains the date and time of the event and a brief message describing the event. Once the log file reaches the log size limit, the log entry is cleared and optionally emailed to the SonicWALL SSL VPN administrator.

The log table size can be specified on the **System > Administration** page under **Default Table Size**.

Column Views

Each log entry displays the following information:

Table 15 Log View Columns

Column	Description
Time	The time stamp displays the date and time of log events in the format *YY*/*MM*/*DD*/*HH*/*MM*/*SS* (Year/Month/Day/Hour/Minute/Second). Hours are displayed in 24-hour clock format. The date and time are based on the local time of the SSL VPN gateway which is configured in the **System > Time** page.
Priority	The level of severity associated with the event. Severity levels can be **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Information**, and **Debug**.
Category	The category of the event message. Categories include Authentication, Authorization & Access, GMS, NetExtender, System, Virtual Assist, and Web Application Firewall.
Source	The Source IP address shows the IP address of the appliance of the user or administrator that generated the log event. The source IP address may not be displayed for certain events, such as system errors.
Destination	The Destination IP address shows the name or IP address of the server or service associated with the event. For example, if a user accessed an intranet Web site through the SSL VPN portal, the corresponding log entry would display the IP address or Fully Qualified Domain Name (FQDN) of the Web site accessed.
User	The name of the user who was logged into the appliance when the message was generated.
Message	The text of the log message.

Navigating and Sorting Log View Table Entries

The **Log View** page provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the facilities described in the following table:

Table 16 Log Table Navigation Facilities

Navigation Button	Description
Find	Enables you to search for a log containing a specified setting based on a criteria type you select in the criteria list. Criteria includes Time, Priority, Source, Destination, and User. Search results list out the results in various orders depending upon the criteria type.
Exclude	Enables you to display all log entries but the type specified in the criteria list.
Reset	Resets the listing of log entries to their default sequence after you have displayed them in an alternate way, using search buttons.

Log > View Buttons

The **Log > View** page also contains options that allow the administrator to send, save log files for external viewing or processing.

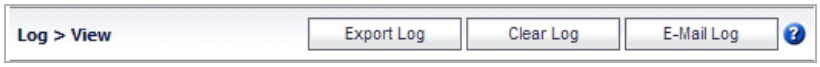


Table 17 Log rendering options

Button	Action
Export Log	Exports the current log contents to a text-based file. Local log contents are cleared after an export log command.
Clear Log	Clears the current log contents.
E-Mail Log	Emails the current log contents to the address specified in the **Log > Settings** screen. Local log contents are cleared after an email log command.

Viewing Logs

The **Log > View** page allows the administrator to view the SonicWALL SSL VPN event log. The SonicWALL SSL-VPN appliance maintains an event log for tracking system events, for example, unsuccessful login attempts, NetExtender sessions, and logout events. This log can be viewed in the **Log > View** page, or it can be automatically sent to an email address for convenience and archiving.

The SonicWALL SSL-VPN appliance can store 250 Kilobytes of log data or approximately 1,000 log messages. Logs are displayed in a sortable, searchable table. The SonicWALL appliance can alert you of events, such as a successful login or an exported configuration. Alerts can be immediately emailed, either to an email address or to an email pager. Each log entry contains the date and time of the event and a brief message describing the event. Once the log file reaches the log size limit, the log entry is cleared and optionally emailed to the SonicWALL SSL VPN administrator.

Each log entry displays the following information:

Table 18 Log View Columns

Column	Description
Time	Displays the date and time of log events in the format *YY*/*MM*/*DD*/*HH*/*MM*/*SS* (Year/Month/Day/Hour/Minute/Second). Hours are displayed in 24-hour clock format. The date and time are based on the local time of the SonicWALL SSL VPN gateway which is configured in the **System > Time** page.
Priority	Displays the level of severity associated with the event. Severity levels can be **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Information**, and **Debug**.
Category	The category of the event message.
Source	Displays the IP address of the appliance of the user or administrator that generated the log event. The source IP address may not be displayed for certain events, such as system errors.
Destination	Displays the name or IP address of the server or service associated with the event. For example, if a user accessed an Internet Web site through the SonicWALL SSL VPN portal, the corresponding log entry would display the IP address or Fully Qualified Domain Name (FQDN) of the Web site accessed.
User	The name of the user who was logged into the appliance when the message was generated.
Message	The text of the log message.

Emailing Logs

The **E-mail Log** button allows the administrator to immediately send and receive a copy of the SonicWALL SSL VPN event log. This feature is useful archiving email and in testing email configuration and email filters for multiple SSL-VPN units. To use the **E-mail Log** feature, perform the following tasks:

Step 1 Navigate to **Log > View**.

Step 2 Click the **E-mail Log** button.

Step 3 You will see the message **Log has been successfully sent**.

Note If you receive an error message, verify that the administrator email and mail server information has been specified in the **Email Logging and Alerts** section of the **Log > Settings** page. For instructions on configuring the administrator email, refer to “Configuring Log Settings” on page 259**.**

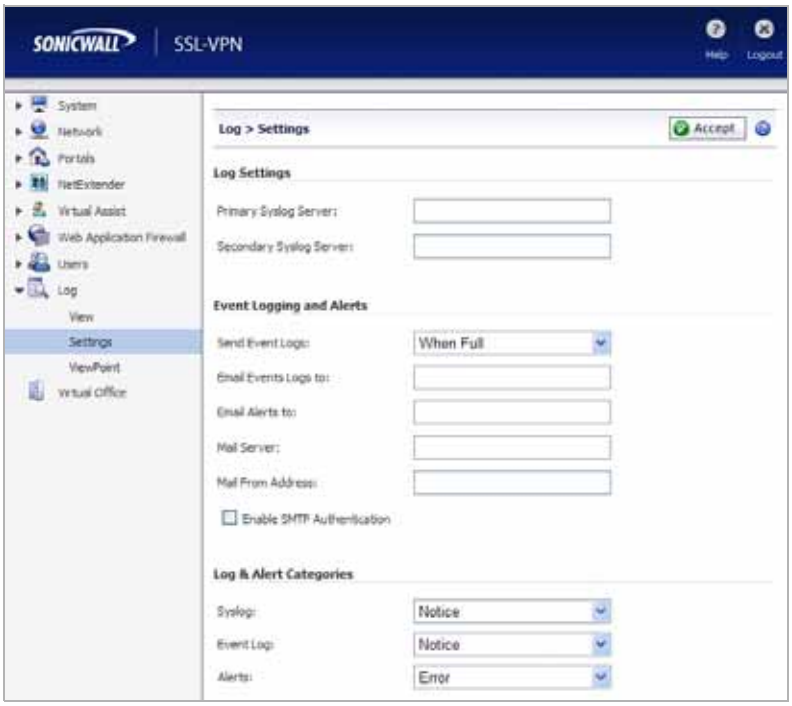
Log > Settings

This section provides an overview of the **Log > Settings** page and a description of the configuration tasks available on this page.

Log > Settings Overview

The **Log > Settings** page allows the administrator to configure log alert and syslog server settings. Syslog is an industry-standard logging protocol that records system and networking activity. The syslog messages are sent in WELF (WebTrends Enhanced Log Format), so most standard firewalls and networking reporting products can accept and interpret the log files. The syslog service transmits syslog messages to external syslog server(s) listening on UDP port 514.

Figure 30 Log > Settings Page



Log Settings

The Log Settings section allows the administrator to specify the primary and secondary Syslog server.

Event Logging and Alerts

The Event Logging and Alerts section allows the administrator to configure email alerts by specifying the email address for logs to be sent to, the mail server, mail from address, and the frequency to send alert emails. You can schedule a day and hour at which to email the event log, or schedule a weekly email, or send the email when the log is full. You can enable SMTP authentication and configure the user name and password along with the SMTP port.

Log & Alert Categories

The Log & Alert Categories section allows the administrator to select categories for Syslog, Event log, and Alerts. The categories are: emergency, alert, critical, error, warning, notice, info, and debug.

Configuring Log Settings

To configure log and alert settings, complete the following steps:

Step 1 To begin configuring event log, syslog and alert settings, navigate to the **Log > Settings** page.

Step 2 Enter the IP address or fully qualified domain name (FQDN) of your syslog server in the **Primary Syslog Server** field. Leave this field blank if you do not require syslog logging.

Step 3 If you have a backup or second syslog server, enter the server's IP address or domain name in the **Secondary Syslog Server** field.

Step 4 Designate when log files will be cleared and emailed to an administrator in the **Send Event Logs** field. If the option **When Full** is selected, the event log will be emailed and then cleared from when the log file is full. If **Daily** is selected, select the hour at which to email the event log. If **Weekly** is selected, select the day of the week and the hour. If **Daily** or **Weekly** are chosen, the log file will still be sent if the log file is full before the end of the period. In the **Log > View** page, you can click the **Clear Log** button to delete the current event log. The event log will not be emailed in this case.

Step 5 To receive event log files via email, enter your full email address (username@domain.com) in the **Email Event Logs to** field in the Event Logging and Alerts region. The event log file will be emailed to the specified email address before the event log is cleared. If this field is left blank, log files will not be emailed.

Step 6 To receive alert messages via email, enter your full email address (username@domain.com) or an email pager address in the **Email Alerts to** field. An email will be sent to the email address specified if an alert event occurs. If this field is left blank, alert messages will not be emailed.

Note Define the type of events that will generate alert messages in the Log and Alert Categories region of the **Log > Settings** page.

Step 7 To email log files or alert messages, enter the domain name or IP address of your mail server in the **Mail Server** field. If this field is left blank, log files and alert messages will not be emailed.

Step 8 Specify a **Mail From Address** in the corresponding field. This address appears in the from field of all log and alerts emails.

Step 9 To use SMTP authentication when sending log files, select the **Enable SMTP Authentication** checkbox. The display will change to expose related fields. Enter the user name, password, and the SMTP port to use. The default port is 25.

Step 10 Define the severity level of log messages that will be identified as syslog, event log or alert messages in the **Log & Alert Categories** region of the **Log > Settings** page. Log categories are organized from most to least critical. If a category is selected for a specific logging service, then that log category and more critical events will be logged. For example, if the Error radio button is selected for the Event Log service, then all Emergency, Alert, Critical, and Error events will be stored in the internal log file.

Step 11 Click **Accept** to update your configuration settings.

Configuring the Mail Server

In order to receive notification email and to enable to the One Time Password feature, it is imperative that you configure the mail server from the **Log > Settings** page. If you fail to configure your mail server prior to using the One Time Password feature, you will receive an error message:

For information about configuring the One Time Password feature, refer to "One Time Password Overview" section on page 28.

To configure the mail server, perform the following steps:

Step 1 Log in to the SonicWALL SSL VPN management interface using administrator credentials.

Step 2 Navigate to **Log > Settings**.

Step 3 Type the email address where you want logs sent to in the **Email Events Logs to** field.

Step 4 Type the email address where you want alerts sent to in the **Email Alerts to** field.

Step 5 Type the IP address for the mail server you will be using in the **Mail Server** field.

Step 6 Type the email address for outgoing mail from your SonicWALL SSL-VPN appliance in the **Mail From Address** field.

Step 7 Click **Accept** in the upper right-hand corner.

Log > Categories

This section provides an overview of the **Log > Categories** page and a description of the various categories of event messages that can be viewed in the log. This page allows for each category to be enabled or disabled by the administrator. This capability can be particularly helpful when used to filter the log during the debug process.

Administrators can enable or disable checkboxes for each of the following log categories:

- Authentication
- Authorization & Access
- GMS
- NetExtender
- System
- Virtual Assist
- Web Application Firewall

Once all selections have been made, click **Accept** in the upper right corner of the screen to finish configuring the desired categories.

Log > ViewPoint

This section provides an overview of the **Log > ViewPoint** page and a description of the configuration tasks available on this page.

Log > ViewPoint Overview

The **Log > ViewPoint** page allows the administrator to add the SonicWALL SSL-VPN appliance to a ViewPoint server for installations that have SonicWALL ViewPoint available, or are managed by the SonicWALL Global Management System (GMS) appliance management software. This feature requires a ViewPoint license key.

Note SonicWALL Analyzer can be connected to SSL-VPN 2000 and 4000 appliances. Use the **Log > ViewPoint** page to set up the Analyzer connection (in addition to the configuration changes made on the Analyzer). In later versions of SonicWALL SRA SSL-VPN, the **Log > ViewPoint** page has been updated to **Log > Analyzer**.

ViewPoint is an integrated appliance management solution that:

- Creates dynamic, web-based reports of SSL-VPN appliance and remote access activity
- Generates both real-time and historical reports to provide a complete view of activity through your SonicWALL SSL-VPN Appliance
- Enables remote access monitoring
- Enhances network security
- Helps you to anticipate future bandwidth needs

Tip For more information about monitoring your SonicWALL appliances with ViewPoint, visit http://www.sonicwall.com/us/Centralized_Management_and_Reporting.html

Adding a ViewPoint Server

This feature requires a ViewPoint license key. To add the SonicWALL SSL-VPN appliance to a ViewPoint server and enable ViewPoint reporting on your SSL-VPN appliance, complete the following steps:

Step 1 Navigate to the **Log > ViewPoint** page in the SonicWALL SSL VPN Web management interface.

Note If you are using ViewPoint for the first time on this appliance or if you do not have a valid license, the page directs you to the **System > Licenses** page to activate your license.

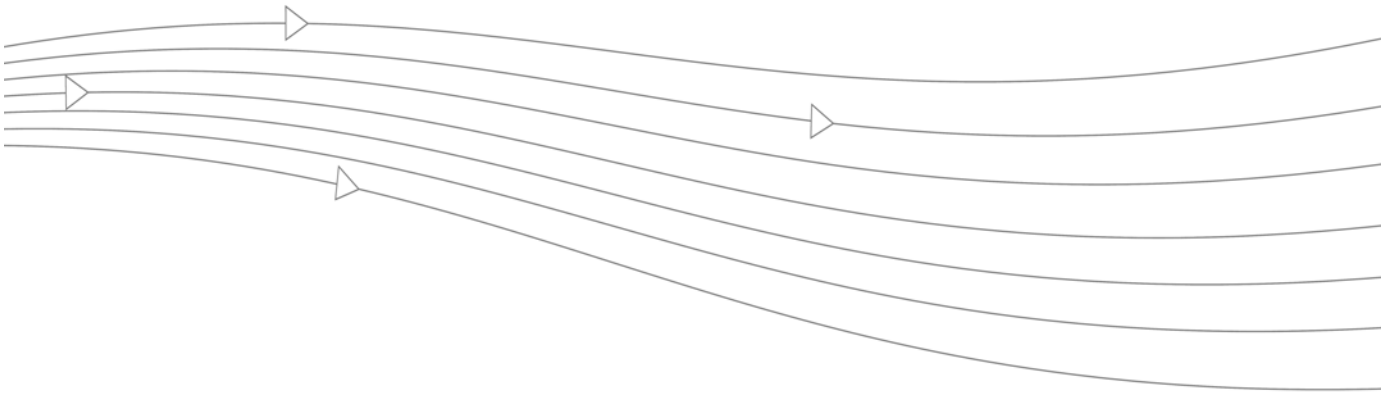
Step 2 In the ViewPoint Settings section, click the **Add** button. The Add ViewPoint Server screen displays.

Step 3 In the Add ViewPoint Server screen, enter the **Hostname or IP Address** of your ViewPoint server.

Step 4 Enter the **Port** which your ViewPoint server communicates with managed devices.

Step 5 Click the **OK** button to add this server.

Step 6 To start ViewPoint report logging for the server you just added, select the **Enable ViewPoint** checkbox.



Chapter 11: Virtual Office Configuration

This chapter provides information and configuration tasks specific to the **Virtual Office** page on the SonicWALL SSL VPN Web-based management interface.

This chapter contains the following section:

Virtual Office

This section provides an overview of the **Virtual Office** page and a description of the configuration tasks available on this page.

Virtual Office Overview

The **Virtual Office** option is located in the navigation bar of the SonicWALL SSL VPN management interface.

The **Virtual Office** option launches the Virtual Office user portal in a separate Web browser window. The Virtual Office is a portal that users can access in order to create and access bookmarks, file shares, NetExtender sessions, and Virtual Assist.

Using the Virtual Office

To use the Virtual Office, perform the following tasks:

Step 1 From the SonicWALL SSL VPN Web-based management interface, click **Virtual Office** in the navigation bar.

Step 2 A new browser window opens to the Virtual Office home page.

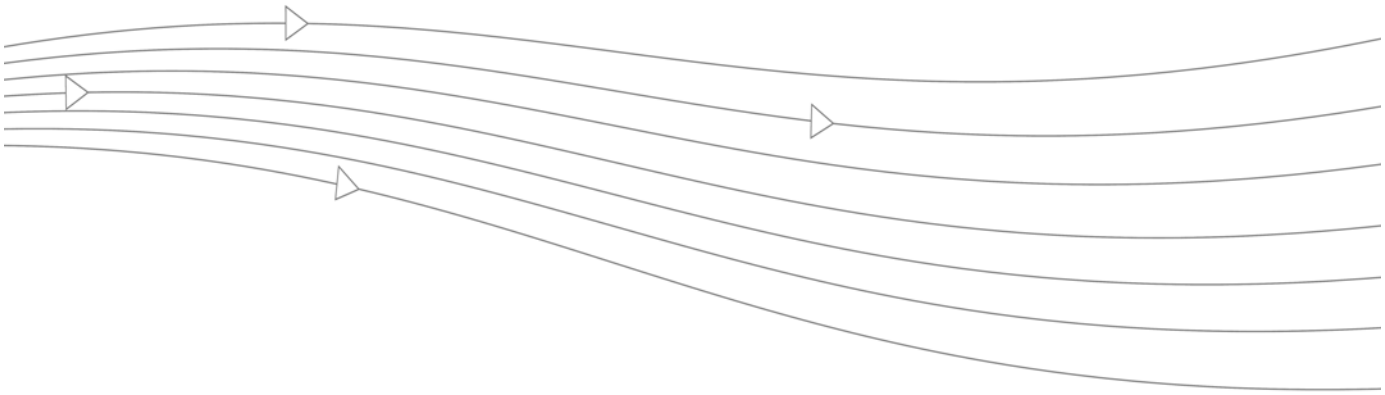
Note When you launch the Virtual Office from the Web-based management interface, you will be automatically logged in with your administrator credentials.

Step 3 From the Virtual Office home page, you can:

- Launch and install NetExtender
- Use File Shares
- Launch a Virtual Assist session
- Add and configure bookmarks
- Add and configure bookmarks for offloaded portals
- Follow bookmark links
- Import certificates
- Get Virtual Office help
- Configure a system for Virtual Access mode, if allowed by administrator
- Configure passwords
- Configure single sign-on options

Note For detailed configuration information about the Virtual Office user portal and these tasks, refer to the *SonicWALL SSL-VPN User's Guide*, available on the Secure Remote Access pages of the SonicWALL support Web site at http://www.sonicwall.com/us/Support.html.

Tip The **Logout** button will not appear in the Virtual Office when you are logged on as an administrator. To log out, you must close the browser window.



Appendix A: Online Help

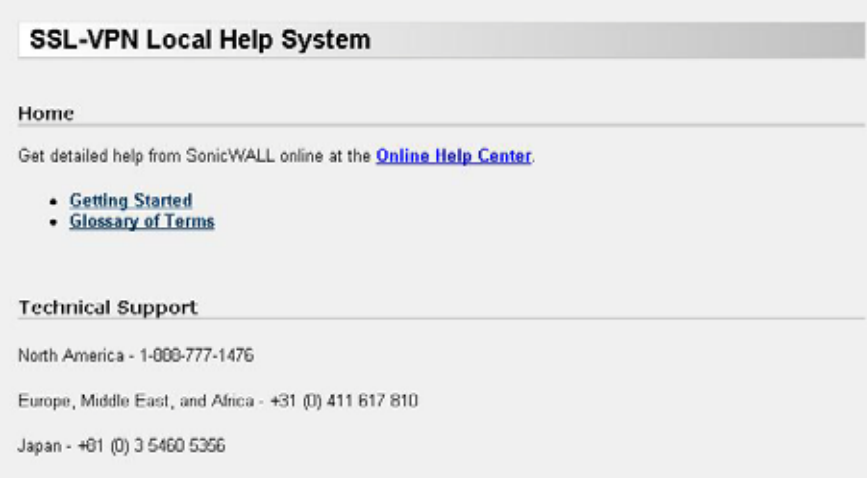
This appendix describes how to use the **Online Help** on the SonicWALL SSL VPN Web-based management interface. This appendix also contains information about context-sensitive help.

This appendix contains the following sections:

Online Help

The **Online Help** button is located in upper right corner of the SonicWALL SSL VPN management interface.

The **Online Help** button launches the online help in a separate Web browser. The **Online Help** button links to the main page of the online help document.



Using Context Sensitive Help

Context-sensitive help is available on most pages of the SonicWALL SSL VPN Web-based management interface. Click the context-sensitive help button in the top right corner of the page to get help that corresponds to the SonicWALL SSL VPN management page you are using. Clicking the context-sensitive help button launches a separate browser window to the corresponding documentation.

The same help icon appears next to certain fields and checkboxes throughout the management interface. When you hover your mouse cursor over one of these help icons, a tooltip is displayed containing important information about configuring the associated option.

Appendix B: Configuring SonicWALL SSL VPN with a Third-Party Gateway

This appendix shows methods for configuring various third-party firewalls for deployment with a SonicWALL SSL-VPN appliance.

This appendix contains the following sections:

Cisco PIX Configuration for SonicWALL SSL-VPN Appliance Deployment

Before you Begin

Make sure you have a management connection to the PIX's console port, or the ability to Telnet/SSH into one of the PIX's interfaces. You will need to know the PIX's global and enable-level passwords in order to access the device and issue changes to the configuration. If you do not have these, contact your network administrator before continuing.

SonicWALL recommends updating the PIX's OS to the most recent version if your PIX can support it. This document was validated on a Cisco PIX 515e running PIX OS 6.3.5 and is the recommended version for interoperation with a SonicWALL SSL-VPN appliance. You will need a valid Cisco SmartNET maintenance contract for your Cisco PIX and a CCO login to obtain newer versions of the PIX OS.

Note The WAN/DMZ/LAN IP addresses used in the deployment method examples below are not valid and will need to be modified to reflect your networking environment.

Note **Recommended Version**: PIX OS 6.3.5 or newer

Management Considerations for the Cisco Pix

Both deployment methods described below use the PIX's WAN interface IP address as the means of external connectivity to the internal SonicWALL SSL-VPN appliance. The PIX has the ability to be managed via HTTP/S, but cannot have their default management ports (80,443) reassigned in the recommended PIX OS version. Because of this, the HTTP/S management interface must be deactivated. To deactivate the HTTP/S management interface, issue the command 'clear http'.

Note If you have a separate static WAN IP address to assign to the SonicWALL SSL-VPN appliance, you do not have to deactivate the HTTP/S management interface on the PIX.

Method One – SonicWALL SSL-VPN Appliance on LAN Interface

Step 1 From a management system, log into the SonicWALL SSL-VPN appliance's management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.

Step 2 Navigate to the **Network > Interfaces** page and click on the configure icon for the X0 interface. On the pop-up that appears, change the X0 address to **192.168.100.2** with a mask of **255.255.255.0**. When done, click on the **OK** button to save and activate the change.

Step 3 Navigate to the **Network > Routes** page and change the Default Gateway to **192.168.100.1** When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 4 Navigate to the **NetExtender > Client Addresses** page. You will need to enter a range of IP addresses for the 192.168.100.0/24 network that are not in use on your internal LAN network; if your network has an existing DHCP server or the PIX is running a DHCP server on its internal interface, you will need to make sure not to conflict with these addresses. For example: enter **192.168.100.201** in the field next to **Client Address Range Begin:**, and enter **192.168.100.249** in the field next to **Client Address Range End:**. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 5 Navigate to the **NetExtender > Client Routes** page. Add a client route for **192.168.100.0**. If there is an entry for **192.168.200.0**, delete it.

Step 6 Navigate to the **Network > DNS** page and enter your internal network's DNS addresses, internal domain name, and WINS server addresses. These are critical for NetExtender to function correctly. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 7 Navigate to the **System > Restart** page and click on the **Restart...** button.

Step 8 Install the SonicWALL SSL-VPN appliance's X0 interface on the LAN network of the PIX. Do not hook any of the appliance's other interfaces up.

Step 9 Connect to the PIX's management CLI via console port, telnet, or SSH and enter configure mode.

Step 10 Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.

Step 11 Issue the command '**access-list sslvpn permit tcp any host x.x.x.x eq www'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 12 Issue the command **'access-list sslvpn permit tcp any host x.x.x.x eq https'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 13 Issue the command '**static (inside,outside) tcp x.x.x.x www 192.168.100.2 www netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 14 Issue the command **'static (inside,outside) tcp x.x.x.x https 192.168.100.2 https netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 15 Issue the command **'access-group sslvpn in interface outside'**

Step 16 Exit config mode and issue the command **'wr mem'** to save and activate the changes.

Step 17 From an external system, attempt to connect to the SonicWALL SSL-VPN appliance using both HTTP and HTTPS. If you cannot access the SonicWALL SSL-VPN appliance, check all steps above and test again.

Final Config Sample – Relevant Programming in Bold:

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
```

```
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
pager lines 24
logging on
logging timestamp
logging buffered warnings
logging history warnings
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
no ip address dmz
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
static (inside,outside) tcp 64.41.140.167 www 192.168.100.2 www netmask
   255.255.255.255 0 0
static (inside,outside) tcp 64.41.140.167 https 192.168.100.2 https netmask
   255.255.255.255 0 0
access-group sslvpn in interface outside
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
   1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
no snmp-server location
no snmp-server contact
snmp-server community SF*&^SDG
no snmp-server enable traps
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 15
```

```
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access. Please log in to continue.
Cryptochecksum:422aa5f321418858125b4896d1e51b89
: end
tenaya#
```

Method Two – SonicWALL SSL-VPN Appliance on DMZ Interface

This method is optional and requires that the PIX have an unused third interface, such as a PIX 515, PIX 525, or PIX 535. We will be using the default numbering scheme of the SonicWALL SSL-VPN appliance.

Step 1 From a management system, log into the SonicWALL SSL-VPN appliance's management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.

Step 2 Navigate to the **Network > Routes** page and make sure the Default Gateway is set to 192.168.200.2 When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 3 Navigate to the **NetExtender > Client Addresses** page. Enter **192.168.200.201** in the field next to **Client Address Range Begin**:, and enter **192.168.200.249** in the field next to **Client Address Range End**:'. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 4 Navigate to the **NetExtender > Client Routes** page. Add a client route for **192.168.100.0** and **192.168.200.0**.

Step 5 Navigate to the **Network > DNS** page and enter your internal network's DNS addresses, internal domain name, and WINS server addresses. These are critical for NetExtender to function correctly. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

Step 6 Navigate to the **System > Restart** page and click on the **Restart...** button.

Step 7 Install the SonicWALL SSL-VPN appliance's X0 interface on the unused DMZ network of the PIX. Do not hook any of the appliance's other interfaces up.

Step 8 Connect to the PIX's management CLI via console port, telnet, or SSH and enter configure mode.

Step 9 Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.

Step 10 Issue the command '**interface ethernet2 auto'** (or whatever interface you will be using)

Step 11 Issue the command '**nameif ethernet2 dmz security4'** (or whatever interface you will be using)

Step 12 Issue the command '**ip address dmz 192.168.200.2 255.255.255.0'**

Step 13 Issue the command **'nat (dmz) 1 192.168.200.0 255.255.255.0 0 0'**

Step 14 Issue the command '**access-list sslvpn permit tcp any host x.x.x.x eq www'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 15 Issue the command **'access-list sslvpn permit tcp any host x.x.x.x eq https'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 16 Issue the command '**access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0 192.168.100.0 255.255.255.0'**

Step 17 Issue the command '**access-list dmz-to-inside permit ip host 192.168.200.1 any'**

Step 18 Issue the command **'static (dmz,outside) tcp x.x.x.x www 192.168.200.1 www netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 19 Issue the command **'static (dmz,outside) tcp x.x.x.x https 192.168.200.1 https netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

Step 20 Issue the command **'static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0'**

Step 21 Issue the command **'access-group sslvpn in interface outside'**

Step 22 Issue the command **'access-group dmz-to-inside in interface dmz'**

Step 23 Exit config mode and issue the command **'wr mem'** to save and activate the changes.

Step 24 From an external system, attempt to connect to the SonicWALL SSL-VPN appliance using both HTTP and HTTPS. If you cannot access the SonicWALL SSL-VPN appliance, check all steps above and test again.

Final Config Sample – Relevant Programming in Bold:

PIX Version 6.3(5)

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0
   192.168.100.0 255.255.255.0
access-list dmz-to-inside permit ip host 192.168.200.1 any
pager lines 24
logging on
logging timestamp
logging buffered warnings
```

```
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.200.2 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
nat (dmz) 1 192.168.200.0 255.255.255.0 0 0
static (dmz,outside) tcp 64.41.140.167 www 192.168.200.1 www netmask
255.255.255.255 0 0
static (dmz,outside) tcp 64.41.140.167 https 192.168.200.1 https netmask
255.255.255.255 0 0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0
access-group sslvpn in interface outside
access-group dmz-to-inside in interface dmz
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 15
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access. Please log in to continue.
Cryptochecksum:81330e717bdbfdc16a140402cb503a77
: end
```

Linksys WRT54GS

The SonicWALL SSL-VPN should be configured on the LAN switch of the Linksys wireless router.

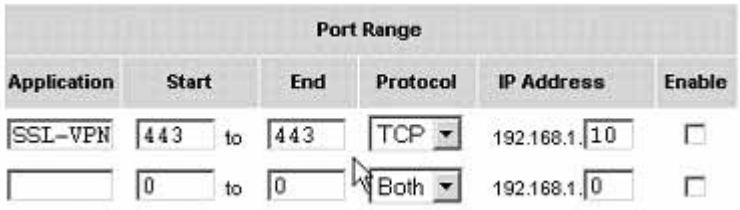
This guide assumes that your Linksys is assigned a single WAN IP, via DHCP by the cable ISP and is using the default LAN IP address scheme of 192.168.1.0/24.

Note Version 2.07.1 Firmware or newer is recommended for this setup.

To configure your Linksys for operation with the SonicWALL SSL-VPN appliance, you must forward the SSL (443) port to the IP address of the SonicWALL SSL-VPN appliance.

Step 1 Login to the Linksys device.

Step 2 Navigate to the **Applications & Gaming** tab.



11. Enter the following information:

Application	SSL VPN	The name for the port forwarded application.
Port Range Start	443	The starting port number used by the application
Port Range End	443	The ending port number used by the application
Protocol	TCP	The SonicWALL SSL VPN application uses TCP
IP Address	192.168.1.10	The IP address assigned to the SonicWALL SSL-VPN appliance.
Enable	Checked	Select the checkbox to enable the SSL port forwarding

Step 3 With the configuration complete, click the **Save Settings** button on the bottom of the page.

The Linksys is now ready for operations with the SonicWALL SSL-VPN appliance.

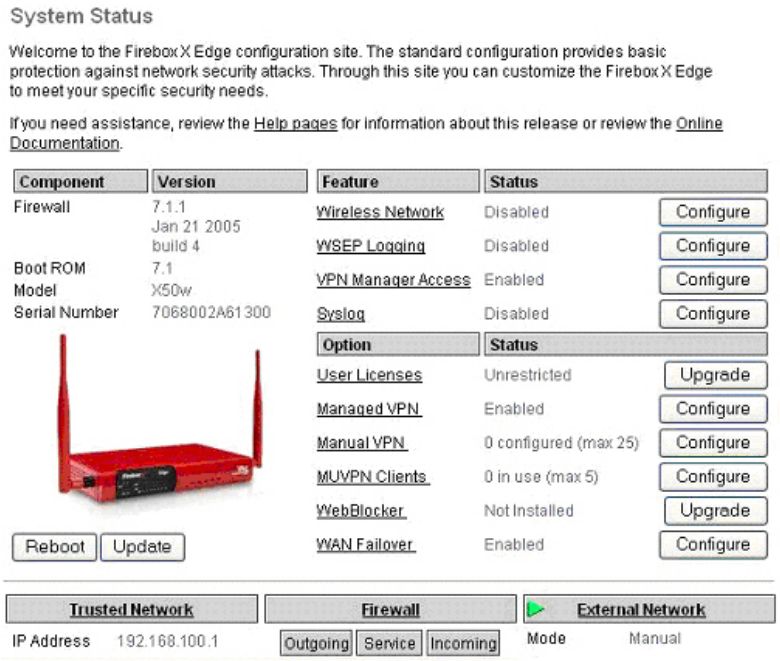
WatchGuard Firebox X Edge

This guide assumes that your WatchGuard Firebox X Gateway is configured with an IP of 192.168.100.1 and your SonicWALL SSL-VPN is configured with an IP of 192.168.100.2.

Note The steps below are similar for WatchGuard SOHO6 series firewall.

Before you get started, take note of which port the WatchGuard is using for management. If the WatchGuard is not being managed on HTTPS (443), perform the following steps. If the WatchGuard is being managed on HTTPS (443) you'll need to first review the notes within this guide.

Step 1 Open browser and enter the IP address of the WatchGuard Firebox X Edge appliance (i.e. 192.168.100.1). Once successful, you'll be brought to the "System Status" page (below).



Step 2 If the WatchGuard's management interface is already configured to accept HTTPS on port 443 you will need to change the port in order to be able to manage both the SonicWALL SSL-VPN and WatchGuard appliances.

Step 3 Navigate to **Administration > System Security**.

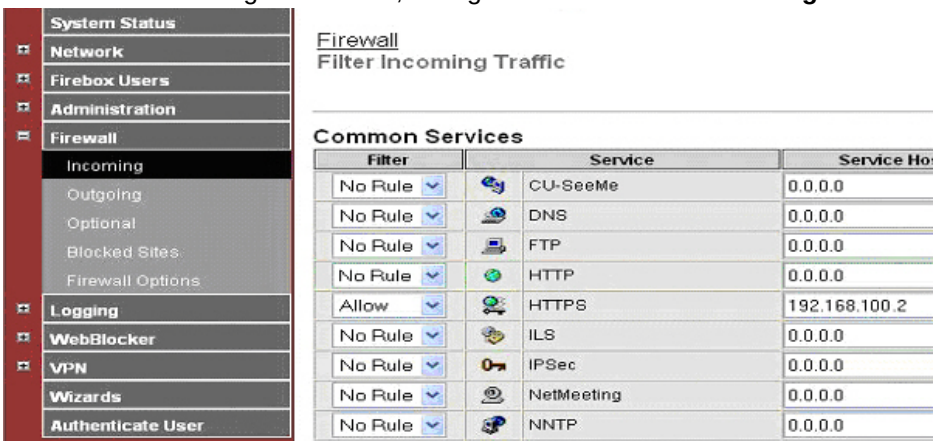
Figure 31 WatchGuard Administration > System Security Dialog Box

Step 4 Uncheck **Use non-secure HTTP instead of secure HTTPS for administrative Web site**.

Step 5 Change the **HTTP Server Port** to 444 and click the **Submit** button.

The WatchGuard will now be managed from the WAN on port 444. It should be accessed as follows: https://<watchguard wan ip>:444

Step 6 In the left-hand navigation menu, Navigate to **Firewall > Incoming**.



Step 7 For the **HTTPS Service**, set **Filter** to Allow and enter the WAN IP of the SonicWALL SSL-VPN appliance (192.168.100.2) in the **Service Host** field.

Step 8 Click the Submit button at the bottom of the page.

Your Watchguard Firebox X Edge is now ready for operations with the SonicWALL SSL-VPN appliance.

NetGear FVS318

This guide assumes that your NetGear FVS318 Gateway is configured with an IP of 192.168.100.1 and your SonicWALL SSL-VPN is configured with an IP of 192.168.100.2.

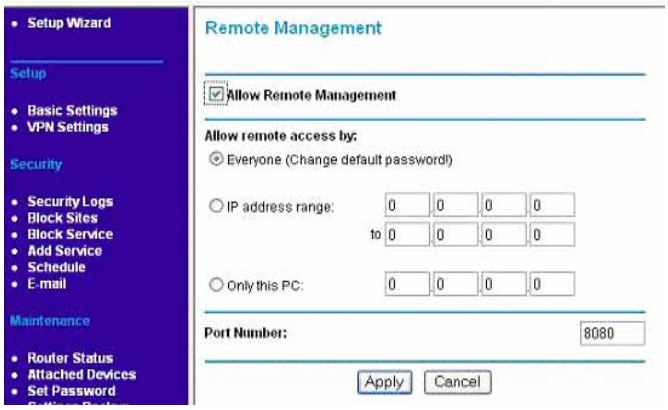
Step 1 Click **Remote Management** from the left-hand index of your Netgear management interface.

In order for the SonicWALL SSL-VPN to function with your Netgear gateway device, you must verify that the NetGear's management port will not conflict with the management port used by the SonicWALL SSL-VPN appliance.

Step 2 Uncheck the **Allow Remote Management** box.

Step 3 Click the **Accept** button to save changes.

Note If Remote Management of the NetGear is desired, you must leave the box checked and change the default port (8080 is recommended)



Step 4 Navigate to **Add Service** in the left-hand navigation.

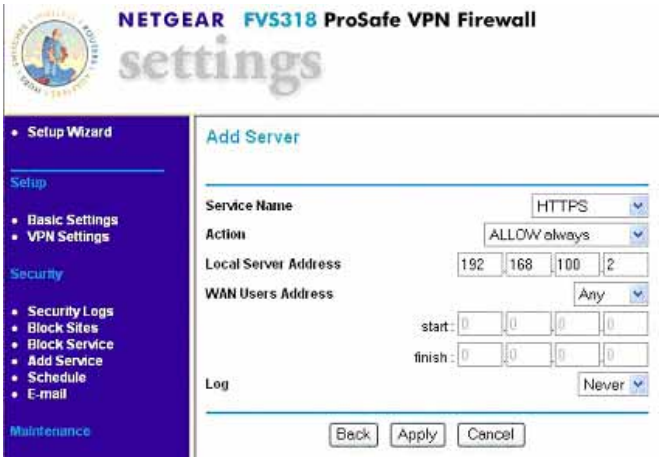
Step 5 Click the **Add Custom Service** button.

Step 6 To create a service definition, enter the following information:

Name	HTTPS
Type	TCP/UDP
Start Port	443
Finish Port	443

Step 7 Navigate to **Ports** in the left-hand navigation.

Step 8 Click the **Add** button.



Step 9 Select HTTPS from the **Service Name** drop-down list.

Step 10 Select ALLOW always in the **Action** drop-down list.

Step 11 Enter the WAN IP address of the SonicWALL SSL-VPN appliance (ex.192.168.100.2) in the **Local Server Address** field.

Step 12 Click Accept to save changes.

Your Netgear gateway device is now ready for operations with the SonicWALL SSL-VPN appliance.

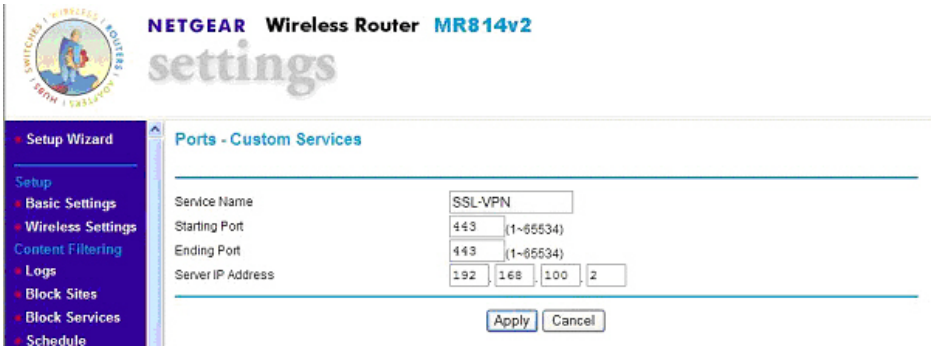
Netgear Wireless Router MR814 SSL configuration

This guide assumes that your NetGear Wireless Router is configured with an IP of 192.168.100.1 and your SonicWALL SSL-VPN is configured with an IP of 192.168.100.2.

Step 1 Navigate to **Advanced > Port Management** in the left-hand index of your Netgear management interface.

Step 2 Click the **Add Custom Service** button in the middle of the page.

Step 3 Enter a service name in the **Service Name** field (ex. SSL VPN)



Step 4 Enter **443** in the **Starting Port** field.

Step 5 Enter **443** in the **Ending Port** field.

Step 6 Enter the WAN IP address of the SonicWALL SSL-VPN appliance (ex.192.168.100.2) in the **Local Server Address** field.

Step 7 Click the **Accept** button

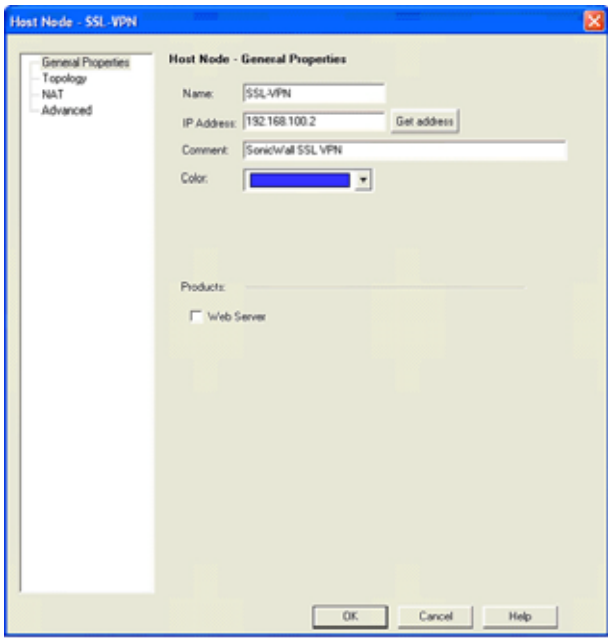
Your Netgear wireless router is now ready for operations with the SonicWALL SSL-VPN appliance.

Check Point AIR 55

Setting up a SonicWALL SSL-VPN with Check Point AIR 55

The first thing necessary to do is define a host-based network object. This is done under the file menu “Manage” and “Network Objects”.

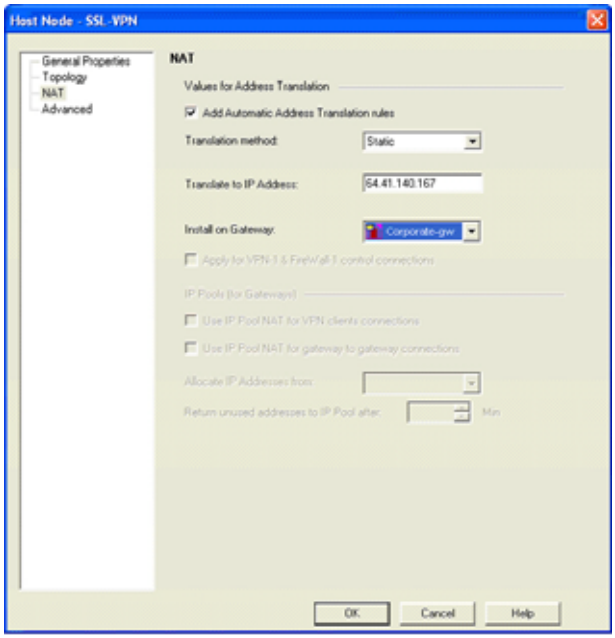
Figure 32 Check Point Host Node Object Dialog Box



Note The object is defined as existing on the internal network. Should you decide to locate the SonicWALL SSL-VPN on a secure segment (sometimes known as a demilitarized zone) then subsequent firewall rules will have to pass the necessary traffic from the secure segment to the internal network.

Next, select the **NAT** tab for the object you have created.

Figure 33 Check Point NAT Properties Dialog Box



Here you will enter the external IP address (if it is not the existing external IP address of the firewall). The translation method to be selected is **static**. Clicking **OK** will automatically create the necessary NAT rule shown below.

Figure 34 Check Point NAT Rule Window

Static Route

Most installations of Check Point AIR55 require a static route. This route will send all traffic from the public IP address for the SonicWALL SSL-VPN to the internal IP address.

#route add 64.41.140.167 netmask 255.255.255.255 192.168.100.2

ARP

Check Point AIR55 contains a feature called auto-ARP creation. This feature will automatically add an ARP entry for a secondary external IP address (the public IP address of the SonicWALL SSL-VPN). If running Check Point on a Nokia security platform, Nokia recommends that users disable this feature. As a result, the ARP entry for the external IP address must be added manually within the Nokia Voyager interface.

Finally, a traffic or policy rule is required for all traffic to flow from the Internet to the SonicWALL SSL-VPN.

Figure 35 Check Point Policy Rule Window

Again, should the SonicWALL SSL-VPN be located on a secure segment of the Check Point firewall, a second rule allowing the relevant traffic to flow from the SonicWALL SSL-VPN to the internal network will be necessary.

Microsoft ISA Server

Deploying a SonicWALL SSL-VPN Behind a Microsoft ISA Server

This section describes how to set up a SonicWALL SSL-VPN appliance behind a Microsoft ISA Server on a Windows Small Business Server (SBS) network. The SBS has an external and an internal network card and ISA is configured in integrated mode. The procedures described in this section have been tested on ISA 2004, but are similar for ISA 2000 and 2006.

Because the SSL-VPN uses the HTTPS protocol on port 443, inbound traffic addressed to port 443 needs to arrive at the SSL-VPN unchanged after traversing the ISA server. However, the ISA server acts as a proxy when you deploy the SSL-VPN as a “Web server” behind it and it does not support HTTPS CONNECT methods.

When ISA intercepts the SSL traffic, it interprets the external HTTP CONNECT method as SSL-TUNNEL traffic with a CONNECT request (a CERN Proxy request), which is an outbound request, and ISA will drop it. When this happens, remote users will not be able to access various client applications including Telnet, SSH, VNC, NetExtender, RDP, and Virtual Assist when connecting through the SonicWall SSL VPN Web portal.

If the SBS is connected to a gateway device or router, the gateway or router must be configured to forward incoming SSL traffic on port 443 to the external network card of the Small Business Server. This port forwarding task is beyond the scope of this section.

Configuring ISA

The SonicWALL SSL-VPN must be published as a **Server** (not a Web Server) within ISA to allow the inbound SSL connection through the ISA firewall.

Configuration Tasks

You will need to perform the following tasks to configure ISA:

- Configure an inbound Protocol Definition for port 443.
- Configure a Server Publishing Rule for the SonicWALL SSL-VPN to make the server available to external users.
- Configure the incoming Web requests listener to ignore inbound SSL traffic.

Configuring a Protocol Definition

To configure an inbound Protocol Definition, perform the following steps on your ISA:

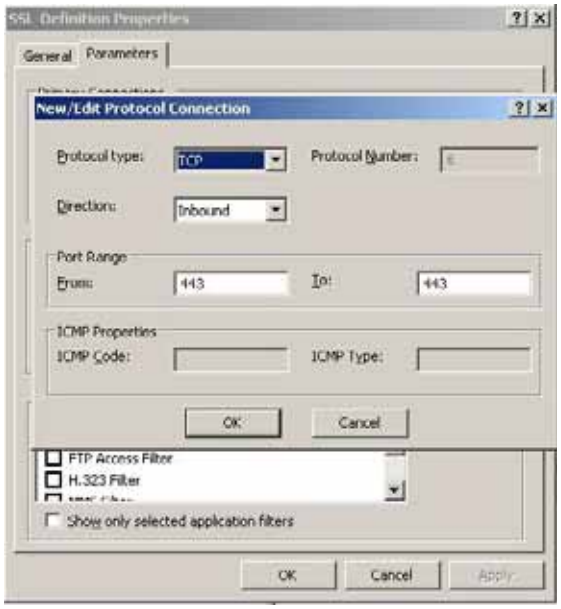
Step 1 In the management interface, create a **Protocol Definition**.

Step 2 Name it **SSL**.

Step 3 Set the **Port number** to **443**.

Step 4 Set the **Protocol type** to **TCP**.

Step 5 Set the **Direction** to **Inbound**.



Step 6 Click **OK**.

Configuring a Server Publishing Rule

As a prerequisite to configuring a Server Publishing Rule, you only need the Protocol Definition configured above. You do not need any of the following configurations:

- Protocol Rule – Although the SonicWALL SSL-VPN is configured as a SecureNAT client, it will not require a protocol rule for outbound traffic. This is because the SSL-VPN does not initiate outbound connections, but only responds to requests made by remote clients.
- Packet Filter –The Server Publishing Rule will open or close ports without the need for a packet filter.
- Site and Content Rule – Responses to inbound requests by a published server are automatically allowed. A site and content rule is not required to allow responses.

To configure a Server Publishing Rule for the SonicWALL SSL-VPN, perform the following steps in the ISA management interface:

Step 1 Start the **Server Publishing Wizard**.

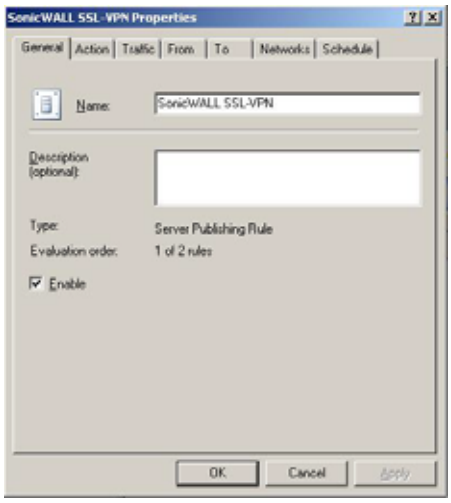
Step 2 Enter a descriptive name for the server, such as **SonicWALL SSL-VPN**.

Step 3 On the **General** tab in the **SonicWALL SSL-VPN Properties** window, select the **Enable** check box.

Step 4 Click the **Action** tab.

Step 5 Enter the IP address of the SonicWALL SSL-VPN appliance in the **IP address of internal server** field.

Step 6 Enter **SSL** as the **Mapped server protocol**. This is the **SSL** Protocol Definition created previously.



Step 7 Click **OK**.

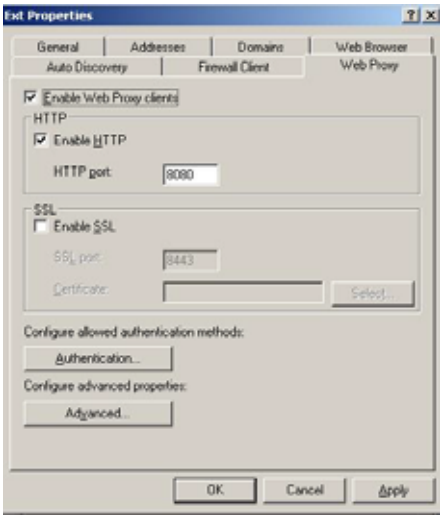
Disabling the Incoming Web Requests Listeners

The default behavior of ISA is to redirect all incoming Web requests on port 80 and 443 to the Web Proxy Service instead of allowing them to pass through to the SonicWALL SSL-VPN. In order to allow traffic arriving on port 443 to reach the SonicWALL, you must disable the Web requests listeners on the ISA server.

To disable the incoming Web requests listeners, perform the following steps:

Step 1 In the ISA server **Properties** window, click the **Web Proxy** tab (**Incoming Web Requests** tab on ISA 2000).

Step 2 In the **SSL** section, clear the **Enable SSL** check box. (On ISA 2000, in the **Identification** section, clear the **Enable SSL listeners** check box.)



Step 3 Click **OK**.

Appendix C: Use Cases

This appendix provides the following use cases:

Importing CA Certificates on Windows

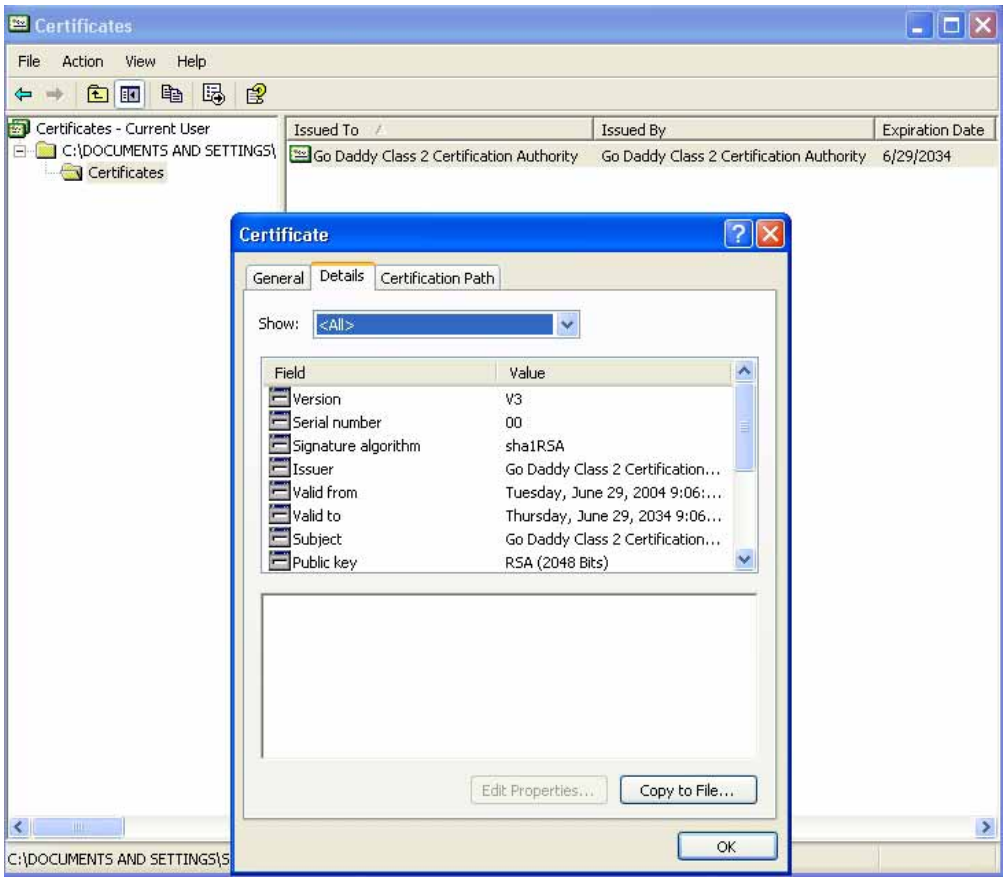
Two certificates are imported in this use case, a goDaddy certificate and a server certificate. See the following sections:

Importing a goDaddy Certificate on Windows

In this use case, we format a goDaddy Root CA Certificate on a Windows system and then import it to our SonicWALL SSL-VPN.

Step 1 Double-click on the **goDaddy.p7b** file to open the Certificates window, and navigate to the goDaddy certificate.
The .p7b format is a PKCS#7 format certificate file, a very common certificate format.

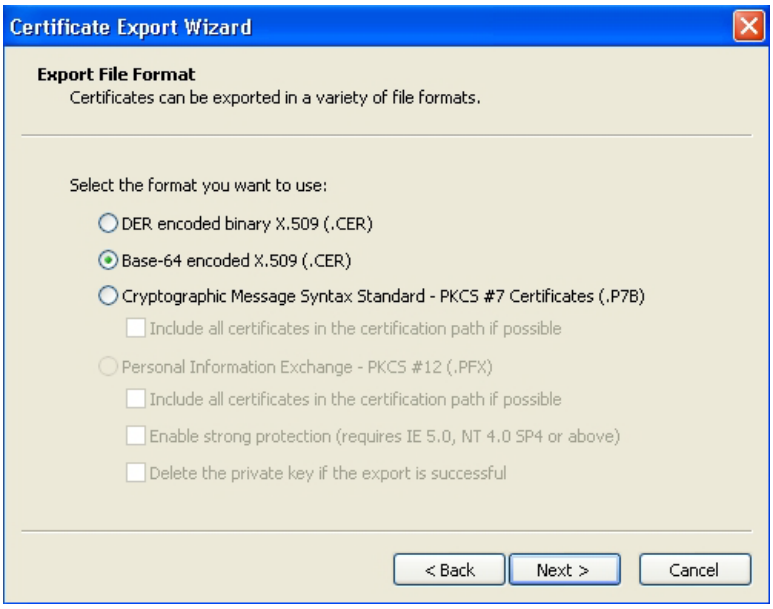
Step 2 Double-click the certificate file and select the **Details** tab.



Step 3 Click **Copy to File**. The Certificate Export Wizard launches.

Step 4 In the Certificate Export Wizard, click **Next**.

Step 5 Select **Base-64 encoded X.509 (.CER)** and then click **Next**.



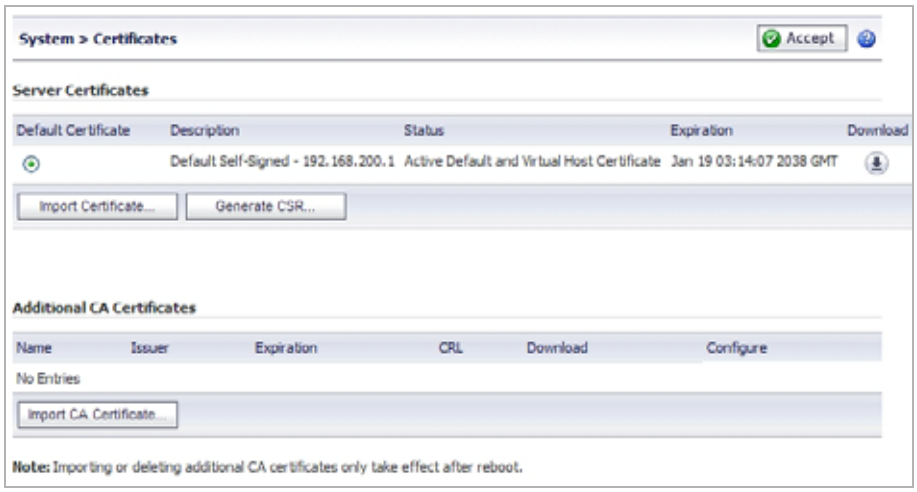
Step 6 In the File to Export screen, type the file name in as **goDaddy.cer** and then click **Next**.

Step 7 In the Completing the Certificate Export Wizard screen, verify the path and format and then click **Finish**.

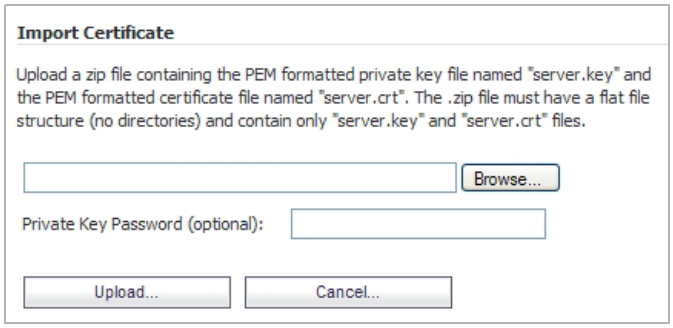
Step 8 Click **OK** in the confirmation dialog box.

The certificate is exported in base-64 encoded format. You can view it in a text editor.

Step 9 In the SonicWALL SSL-VPN management interface, navigate to **System > Certificates**.

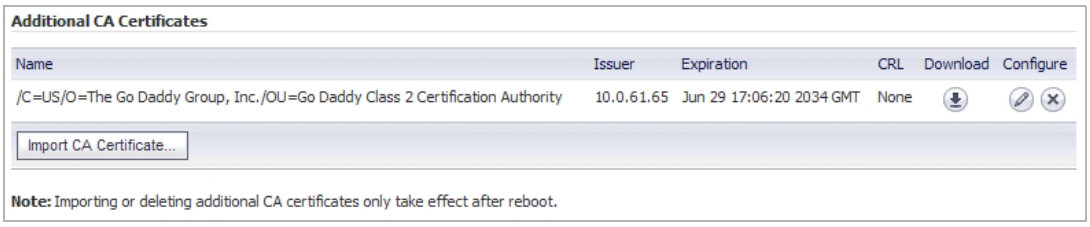


Step 10 In the **Additional CA Certificates** section, click **Import CA Certificate**. The Import Certificate window appears.



Step 11 In the Import Certificate window, click **Browse** and navigate to the **goDaddy.cer** file on your Windows system and double-click it.

Step 12 Click **Upload**. The certificate will be listed in the **Additional CA Certificates** table.



Step 13 Navigate to **System > Restart** and restart the SonicWALL SSL-VPN for the CA certificate to take effect.

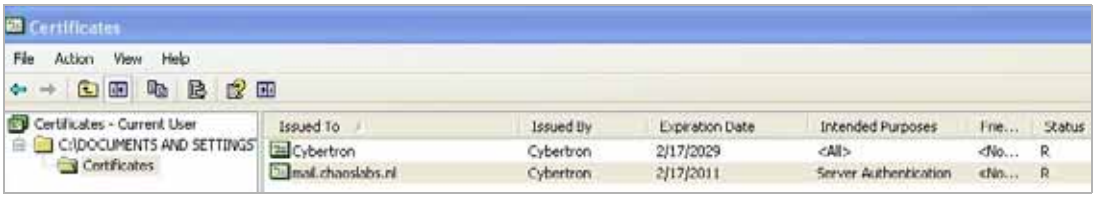
Importing a Server Certificate on Windows

In this use case, we import a Microsoft CA server certificate to a Windows system. In this case, the purpose is to use an SSL certificate for application offloading to a mail server.

The server certificate is **mail.chaoslabs.nl**. This certificate needs to be exported in base-64 format as the **server.crt** file that is put in a .zip file and uploaded as a Server Certificate.

The private key is not included in the **.p7b** file. The private key needs to be exported from wherever it is and saved in a base-64 format and included in a **server.key** file in the .zip file.

Step 1 Double-click on the **mail.chaoslabs.nl.pb7** file and navigate to the certificate.



Step 2 Double-click the certificate file and select the **Details** tab.

Step 3 Click **Copy to File**.

Step 4 In the Certificate Export Wizard, select **Base-64 encoded X.509 (.CER)**.

Step 5 Click **Next** and save the file as **server.crt** on your Windows system.

The certificate is exported in base-64 encoded format.

Step 6 Add the server.crt file to a .zip file.

Step 7 Separately save the private key in base-64 format as **server.key**.

Step 8 Add the **server.key** file to the .zip file that contains **server.crt**.

Step 9 Upload the .zip file to the server as a Server Certificate.

Creating Unique Access Policies for AD Groups

In this use case, we add Outlook Web Access (OWA) resources to the SonicWALL SSL-VPN, and need to configure the access policies for users in multiple Active Directory (AD) groups. We will create a local group for each AD group and apply separate access policies to each local group.

Note The AD Groups feature is only available on SonicWALL SSL-VPN models 2000 and higher.

While Active Directory allows users to be members in multiple groups, the SonicWALL SSL-VPN only allows each user to belong to a single group. It is this group that determines the access policies assigned to the user.

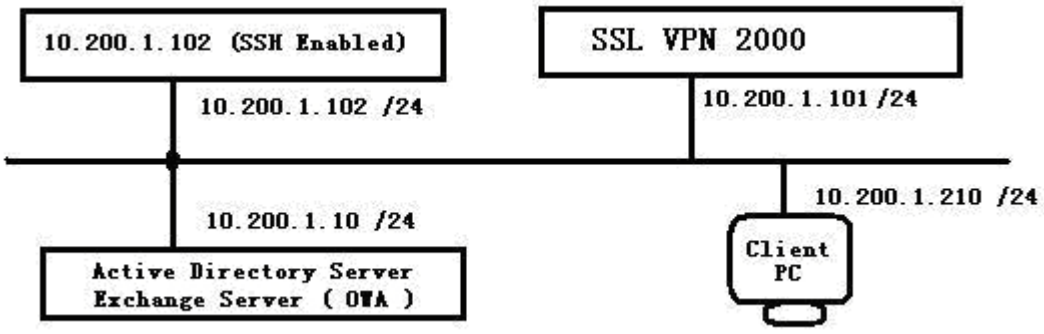
When importing a user from AD, the user will be placed into the local SSL-VPN group with which they have the most AD groups in common. For example: Bob belongs to the Users, Administrators, and Engineering AD groups. If one SSL-VPN group is associated with Users, and another is associated with both Administrators and Engineering, Bob will be assigned to the SSL-VPN group with both Administrators and Engineering because it matches more of his own AD groups.

The goal of this use case is to show that SonicWALL SSL-VPN firmware supports group-based access policies by configuring the following:

- Allow Acme Group in Active Directory to access the 10.200.1.102 server using SSH
- Allow Mega Group in Active Directory to access Outlook Web Access (OWA) at 10.200.1.10
- Allow IT Group in Active Directory to access both SSH and OWA resources defined above
- Deny access to these resources to all other groups

This example configuration is provided courtesy of Vincent Cai, June 2008.

Figure 36 Network Topology



Perform the tasks in order of the following sections:

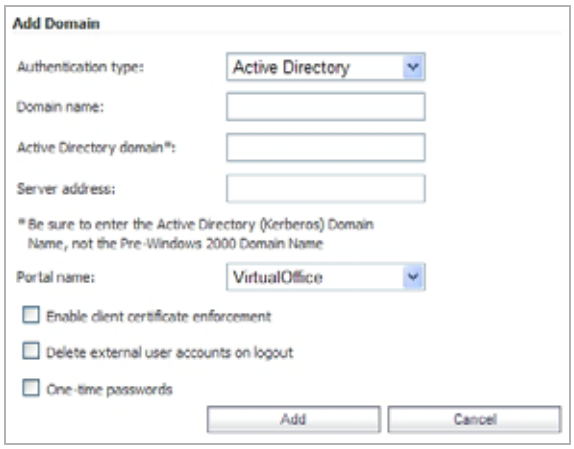
- “Creating the Active Directory Domain” on page 296
- “Adding a Global Deny All Policy” on page 297
- “Creating Local Groups” on page 298
- “Adding the SSHv2 PERMIT Policy” on page 300
- “Adding the OWA PERMIT Policies” on page 301
- “Verifying the Access Policy Configuration” on page 303

Creating the Active Directory Domain

This section describes how to create the SonicWALL SSL-VPN Local Domain, SNWL_AD. SNWL_AD is associated with the Active Directory domain of the OWA server.

Step 1 Log in to the SonicWALL SSL-VPN management interface and navigate to the **Portals > Domains** page.

Step 2 Click **Add Domain**. The Add Domain window appears.



Step 3 In the **Authentication type** drop-down list, select **Active Directory**.

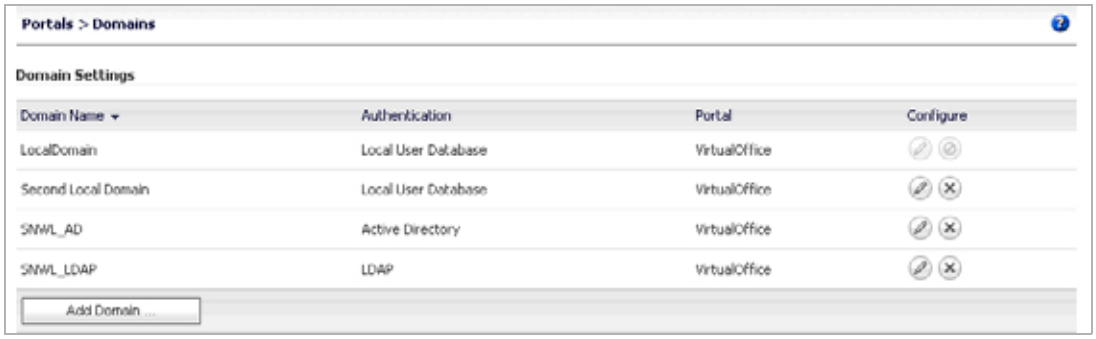
Step 4 In the **Domain name** field, type **SNWL_AD**.

Step 5 In the **Active Directory domain** field, type the AD domain name, **in.loraxmfg.com**.

Step 6 In the **Server address** field, type the IP address of the OWA server, **10.200.1.10**.

Step 7 Click **Add**.

Step 8 View the new domain in the **Portals > Domains** page.



Adding a Global Deny All Policy

This procedure creates a policy that denies access to the OWA resources to all groups, except groups configured with an explicit Permit policy.

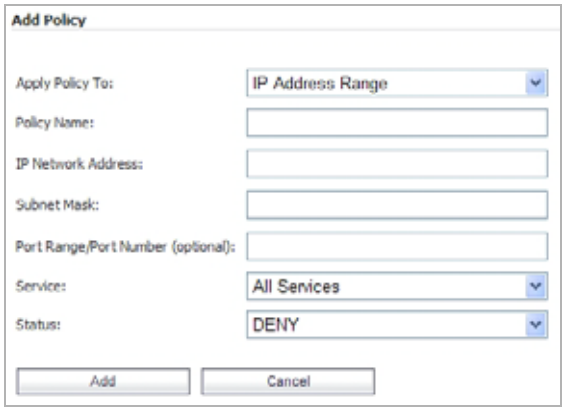
The SonicWALL SSL-VPN default policy is **Allow All**. In order to have more granular control, we add a **Deny All** policy here. Later, we can add **Permit** policies for each group, one at a time.

Step 1 Navigate to the **Users > Local Users** page.

Step 2 Click the **Configure** button in the **Global Policies** row. The **Edit Global Policies** window appears.

Step 3 In the **Edit Global Policies** window, click the **Policies** tab.

Step 4 Click **Add Policy**. The Add Policy window appears.



Step 5 Select **IP Address Range** from the **Apply Policy To** drop-down list.

Step 6 In the **Policy Name** field, type the descriptive name **Deny All**.

Step 7 In the **IP Network Address** field, type the network address, **10.200.1.0**.

Step 8 In the **Subnet Mask** field, type the mask in decimal format, **255.255.255.0**.

Step 9 In the **Service** drop-down list, select **All Services**.

Step 10 In the **Status** drop-down list, select **DENY**.

Step 11 Click **Add**.

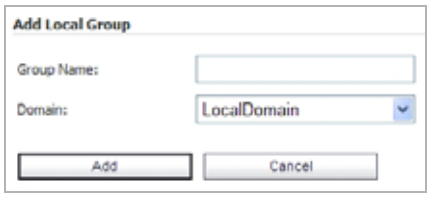
Step 12 In the **Edit Global Policies** window, verify the **Deny All** policy settings and then click **OK**.

Creating Local Groups

This procedure creates Local Groups that belong to the SNWL_AD domain on the SSL-VPN. We create one local group for each Active Directory group.

Adding the Local Groups

Step 1 Navigate to the **Users > Local Groups** page and click **Add Group**. The **Add Local Group** window appears. We will add three local groups, corresponding to our Active Directory groups.



Step 2 In the **Add Local Group** window, type **Acme_Group** into the **Group Name** field.

Step 3 Select **SNWL_AD** from the **Domain** drop-down list.

Step 4 Click **Add**.

Step 5 On the **Users > Local Groups** page, click **Add Group** to add the second local group.

Step 6 In the Add Local Group window, type **Mega_Group** into the **Group Name** field.

Step 7 Select **SNWL_AD** from the **Domain** drop-down list.

Step 8 Click **Add**.

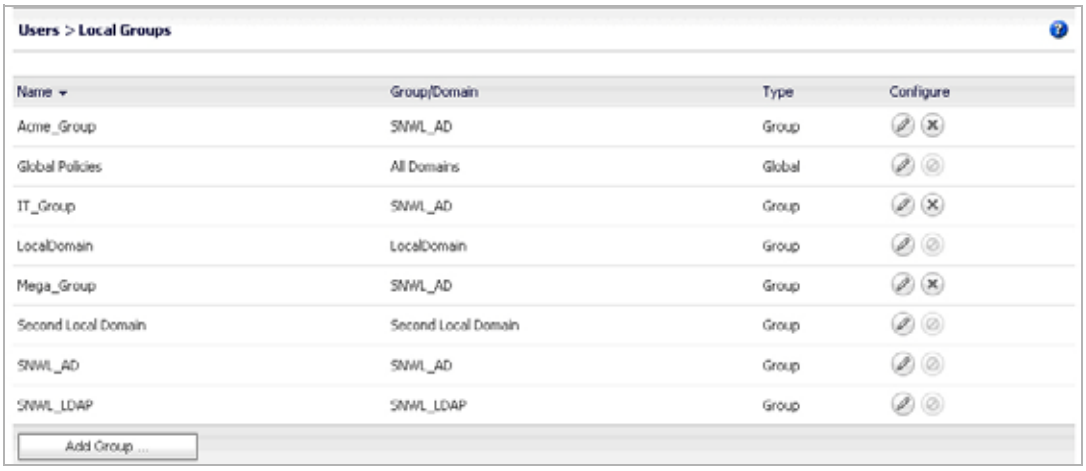
Step 9 On the **Users > Local Groups** page, click **Add Group** to add the second local group.

Step 10 In the Add Local Group window, type **IT_Group** into the **Group Name** field.

Step 11 Select **SNWL_AD** from the **Domain** drop-down list.

Step 12 Click **Add**.

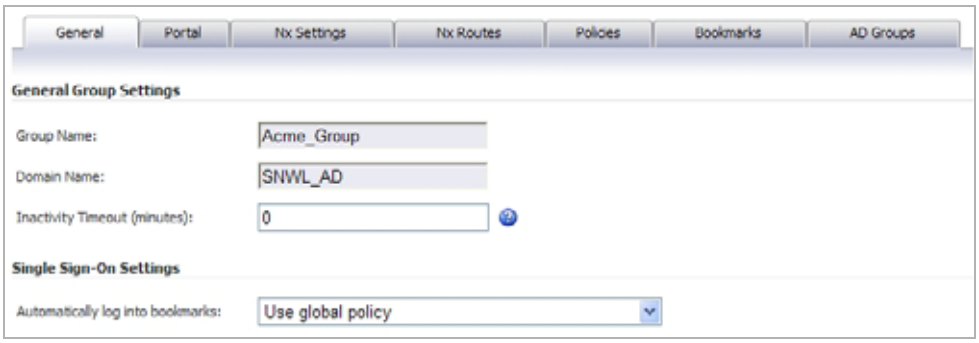
Step 13 View the added groups on the **Users > Local Groups** page.



Configuring the Local Groups

In this procedure we will edit each new local group and associate it with the corresponding Active Directory Group.

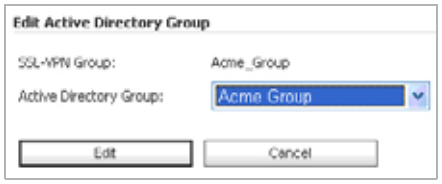
Step 1 Click the **Configure** button in the **Acme_Group** row. The **Edit Group Settings** window appears.



Step 2 In the **Edit Group Settings** window, click the **AD Groups** tab.

Step 3 On the **AD Groups** tab, click the **Add Group** button.

Step 4 In the **Edit Active Directory Group** window, select **Acme Group** from the **Active Directory Group** drop-down list.



Step 5 Click **Edit**.
Acme Group is listed in the **Active Directory Groups** table on the **AD Groups** tab.

Step 6 In the **Edit Group Settings** window, click **OK**.

Step 7 On the **Users > Local Groups** page, click the **Configure** button in the **Mega_Group** row. The **Edit Group Settings** window appears.

Step 8 In the **Edit Group Settings** window, click the **AD Groups** tab and then click the **Add Group** button.

Step 9 In the **Edit Active Directory Group** window, select **Mega Group** from the **Active Directory Group** drop-down list and then click **Edit**.
Mega Group is listed in the **Active Directory Groups** table on the **AD Groups** tab.

Step 10 In the **Edit Group Settings** window, click **OK**.

Step 11 On the **Users > Local Groups** page, click the **Configure** button in the **IT_Group** row. The **Edit Group Settings** window appears.

Step 12 In the **Edit Group Settings** window, click the **AD Groups** tab and then click the **Add Group** button.

Step 13 In the **Edit Active Directory Group** window, select **IT Group** from the **Active Directory Group** drop-down list and then click **Edit**.
IT Group is listed in the **Active Directory Groups** table on the **AD Groups** tab.

Step 14 In the **Edit Group Settings** window, click **OK**.

At this point, we have created the three Local Groups and associated each with its Active Directory Group.

Adding the SSHv2 PERMIT Policy

In this section, we will add the SSHv2 PERMIT policy for both **Acme_Group** and **IT_Group** to access the 10.200.1.102 server using SSH.

This procedure creates a policy for the SonicWALL SSL-VPN Local Group, **Acme_Group**, and results in SSH access for members of the Active Directory group, Acme Group.

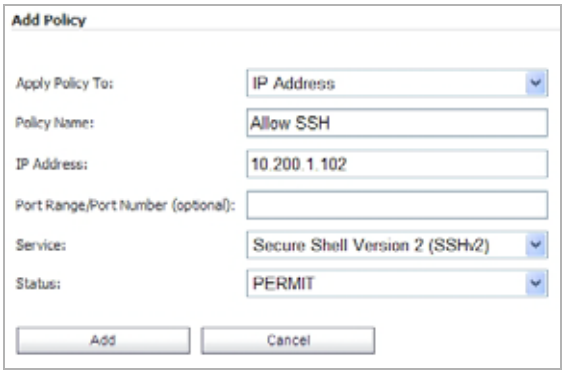
Repeat this procedure for **IT_Group** to provide SSH access to the server for members of the Active Directory group, IT Group.

Step 1 On the **Users > Local Groups** page, click the **Configure** button in the **Acme_Group** row. The **Edit Group Settings** window appears.

Step 2 In the **Edit Group Settings** window, click the **Policies** tab.

Step 3 On the **Policies** tab, click **Add Policy**.

Step 4 In the **Add Policy** window, select **IP Address** in the **Apply Policy To** drop-down list.



Step 5 In the **Policy Name** field, enter the descriptive name, **Allow SSH**.

Step 6 In the **IP Address** field, enter the IP address of the target server, **10.202.1.102**.

Step 7 In the **Services** drop-down list, select **Secure Shell Version 2 (SSHv2)**.

Step 8 In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

Step 9 In the **Edit Group Settings** window, click **OK**.

Adding the OWA PERMIT Policies

In this section, we will add two OWA PERMIT policies for both **Mega_Group** and **IT_Group** to access the OWA service using Secure Web (HTTPS).

This procedure creates a policy for the SonicWALL SSL-VPN Local Group, **Mega_Group**, and results in OWA access for members of the Active Directory group, Mega Group.

To access the Exchange server, adding a PERMIT policy to the **10.200.1.10/exchange** URL Object itself is not enough. Another URL Object policy is needed that permits access to **10.200.1.10/exchweb**, because some OWA Web contents are located in the **exchweb** directory.

Repeat this procedure for **IT_Group** to provide OWA access for members of the Active Directory group, IT Group.

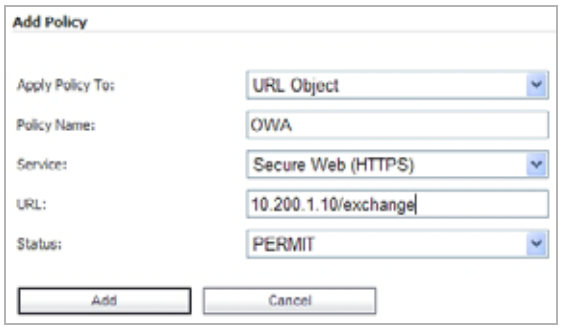
Note In this configuration, members of IT_Group and Mega_Group are denied access to the https://owa-server/public folder, because these groups have access only to the /exchange and /exchweb subfolders.

The OWA policies are applied to Exchange server URL Objects rather than server IP addresses since OWA is a Web service.

Step 1 In the **Users > Local Groups** page, click the **Configure** button in the **Mega_Group** row. We will create **two** PERMIT policies for Mega_Group to allow access to the OWA Exchange server.

Step 2 In the **Edit Group Settings** window, click the **Policies** tab, and then click **Add Policy**.

Step 3 In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.



Step 4 In the **Policy Name** field, enter the descriptive name, **OWA**.

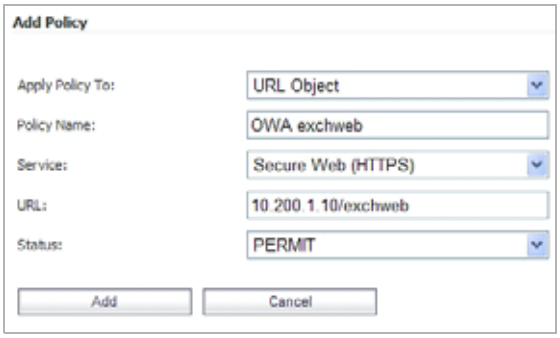
Step 5 In the **Service** drop-down list, select **Secure Web (HTTPS)**.

Step 6 In the **URL** field, enter the URL of the target application, **10.200.1.10/exchange**.

Step 7 In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

Step 8 In the **Edit Group Settings** window on the **Policies** tab, click **Add Policy**.

Step 9 In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.



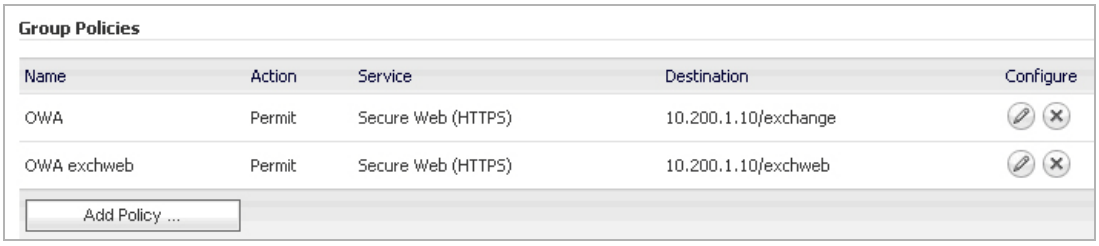
Step 10 In the **Policy Name** field, enter the descriptive name, **OWA exchweb**.

Step 11 In the **Service** drop-down list, select **Secure Web (HTTPS)**.

Step 12 In the **URL** field, enter the URL of the target application, **10.200.1.10/exchweb**.

Step 13 In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

Step 14 In the **Edit Group Settings** window, click **OK**. We are finished with the policies for Mega_Group. Repeat this procedure for IT_Group to provide OWA access for members of the Active Directory group, IT Group.



Verifying the Access Policy Configuration

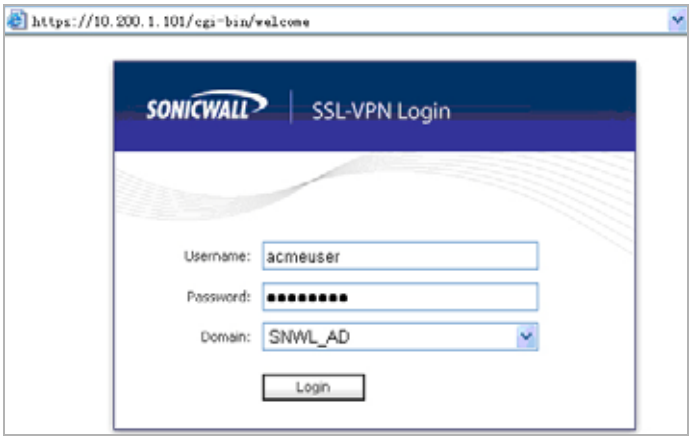
At this point:

- Acme_Group users are allowed to access SSH to 10.200.1.102
- Mega_Group users are allowed to access OWA at 10.200.1.10
- IT_Groups users are allowed to access both SSH and OWA as defined above

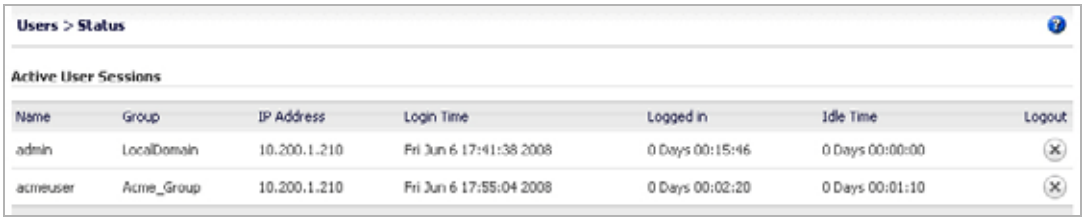
The configuration can be verified by logging in as different AD group members to the SNWL_AD domain on the SonicWALL SSL-VPN, and attempting to access the resources.

Test Result: Try Acmeuser Access

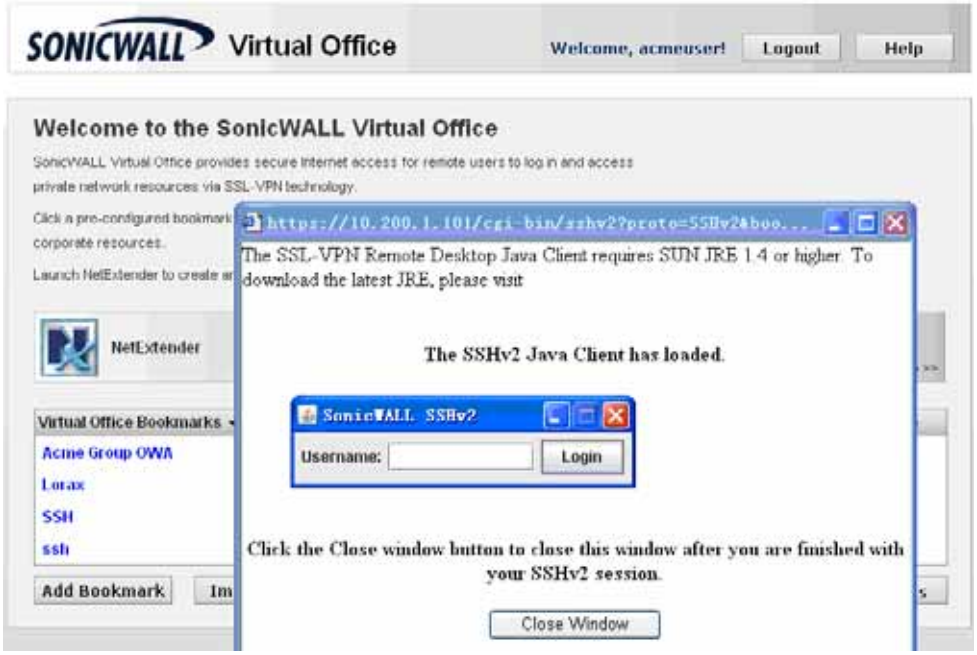
Acmeuser logs into the **SNWL_AD** domain.



The **Users > Status** page shows that **acmeuser** is a member of the local group, **Acme_Group**.



Acmeuser can access SSH, as expected.

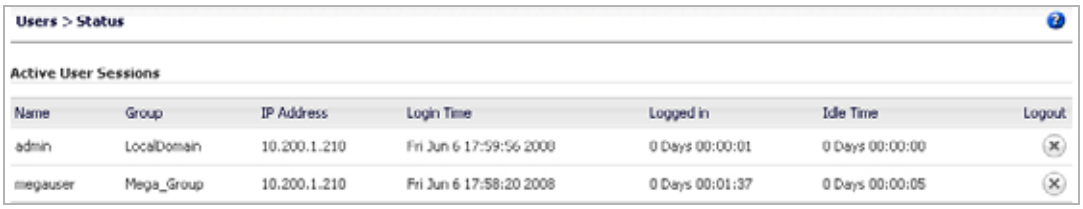


Acmeuser tries to access to other resources like OWA 10.200.1.10, but is denied, as expected.

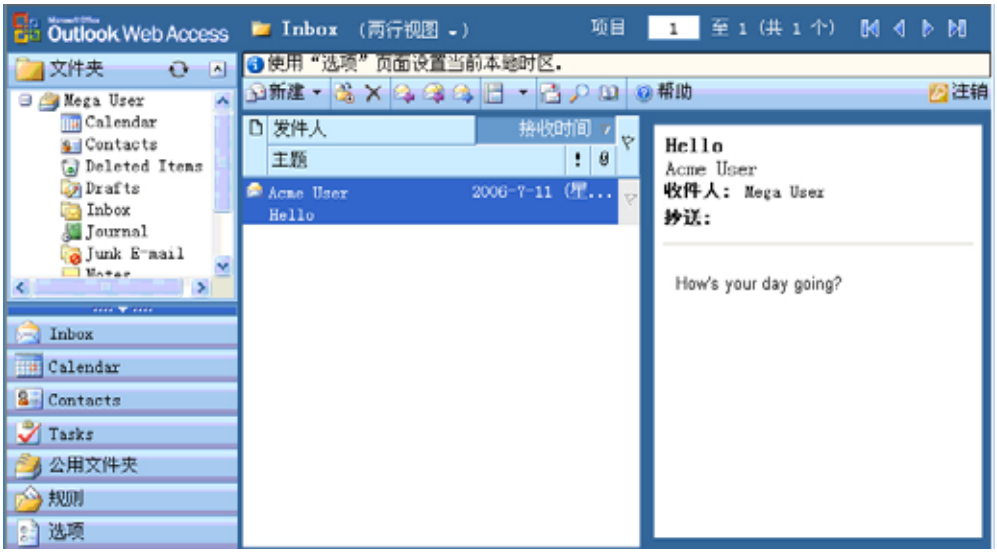
Test Result: Try Megauser Access

Megauser logs into the **SNWL_AD** domain.

The **Users > Status** page shows that **megauser** is a member of the local group, **Mega_Group**.



Megauser can access OWA resources, as expected.

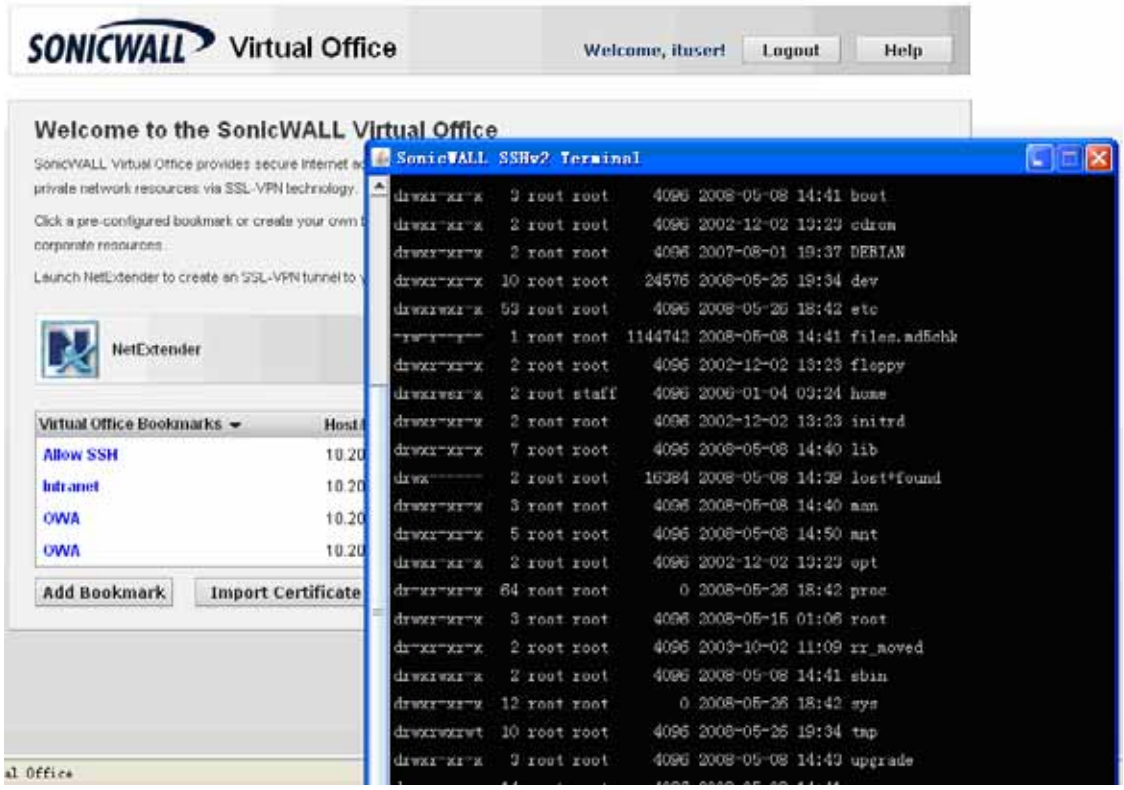


Megauser tries to access SSH, but is denied, as expected.

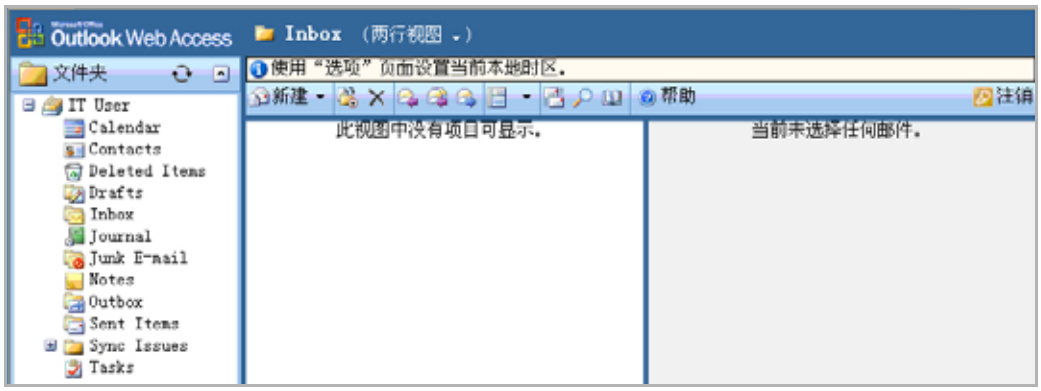
Test Result: Try Ituser Access

Ituser logs into the **SNWL_AD** domain. The **Users > Status** page shows that **ituser** is a member of the local group, **IT_Group**.

Ituser can access SSH to 10.200.1.102, as expected.



ltuser can access OWA resources, as expected.



Appendix D: NetExtender Troubleshooting

This appendix contains a table with troubleshooting information for the SonicWALL SSL VPN NetExtender utility.

Table 19 NetExtender Cannot Be Installed

Problem	Solution
NetExtender cannot be installed.	**1.** Check your OS Version, NetExtender only supports Win2000 or above, Mac OS X 10.5 or above with Apple Java 1.6.0_10 or above, and Linux OpenSUSE in addition to Fedora Core and Ubuntu. An i386-compatible Linux distribution is required, along with Sun Java 1.6.0_10+ **2.** Check that the user has administrator privilege, NetExtender can only install/work under the user account with administrator privileges. **3.** Check if ActiveX has been blocked by Internet Explorer or third-party blockers. **4.** If the problem still exists, obtain the following information and send to support: – The version of SonicWALL SSL VPN NetExtender Adapter from Device Manager. – The log file located at **C:\Program files\SonicWALL\SSL VPN\NetExtender.dbg.** – The event logs in the **Event Viewer** found under the Windows Control Panel **Administrator Tools** folder. Select Applications and System events and use the **Action /Save Log File as…** menu to save the events in a log file.

Table 20 NetExtender Connection Entry Cannot Be Created

Problem	Solution
NetExtender connection entry cannot be created.	1. Navigate to Device Manager and check if the SonicWALL SSL VPN NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again. 2. Navigate to Windows Service manager under **Control Panel > Administrator Tools > Services**. Look for the **Remote Access Auto Connection Manager** and **Remote Access Connection Manager** to see if those two services have been started. If not, set them to automatic start, reboot the machine, and install NetExtender again. 3. Check if there is another dial-up connection in use. If so, disconnect the connection, reboot the machine and install NetExtender again. 4. If problem still exists, obtain the following information and send them to support: – The version of SonicWALL SSL VPN NetExtender Adapter from Device Manager. – The log file located at **C:\Program files\SonicWALL\SSL VPN\NetExtender.dbg**. – The event logs in **Control Panel** > **Administrator Tools** > **Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File as…** menu to save the events in a log file.

Table 21 NetExtender Cannot Connect

Problem	Solution
NetExtender cannot connect.	1. Navigate to Device Manager and check if the SonicWALL SSL VPN NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again. 2. Navigate to Network connections to check if the SonicWALL SSL VPN NetExtender Dialup entry has been created. If not, reboot the machine and install NetExtender again. 3. Check if there is another dial-up connection in use, if so, disconnect the connection and reboot the machine and connect NetExtender again. 4. If problem still exists, obtain the following information and send them to support: – The version of SonicWALL SSL VPN NetExtender Adapter from Device Manager. – The log file located at **C:\Program files\SonicWALL\SSL VPN\NetExtender.dbg**. – The event logs in **Control Panel > Administrator Tools > Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File as…** menu to save the events in a log file.

Table 22 NetExtender BSOD After Connected

Problem	Solution
NetExtender BSOD after connected.	1. Uninstall NetExtender, reboot machine, reinstall the latest version NetExtender. 2. Obtain the following information and send them to support: – The version of SonicWALL SSL VPN NetExtender Adapter from Device Manager. – The log file located at **C:\Program files\SonicWALL\SSL VPN\NetExtender.dbg**. – Windows memory dump file located at **C:\Windows\MEMORY.DMP**. If you can not find this file, then you will need to open System Properties, click the **Startup and Recovery Settings** button under the **Advanced** tab. Select **Complete Memory Dump**, **Kernel Memory Dump** or **Small Memory Dump** in the **Write Debugging Information** drop-down list. Of course, you will also need to reproduce the BSOD to get the dump file. – The event logs in **Control Panel > Administrator Tools > Event Viewer**. Select **Applications and System Events** and use the **Action /Save Log File as…** menu to save the events in a log file.

Appendix E: FAQs

This appendix contains FAQs about SonicWALL SSL VPN.

This appendix contains the following sections:

- Is 2-factor authentication (RSA SecurID, etc) supported?
- Does the SonicWALL SSL-VPN appliance support VoIP?
- Is Syslog supported?
- Does NetExtender support multicast?
- Are SNMP and Syslog supported?
- Does the SonicWALL SSL-VPN appliance have a Command Line Interface (CLI)?
- Can I Telnet or SSH into the SSL-VPN appliance?
- When controlling user access, can I apply permissions on both a domain as well as a Forest basis?
- What does the Web cache cleaner do?
- Why didn't the Web cache cleaner work when I exited the Web browser?
- What does the 'encrypt settings file' checkbox do?
- What does the 'store settings' button do?
- What does the 'create backup' button do?
- What is 'SafeMode'?
- How do I access the SafeMode menu?
- Can I change the colors of the portal pages?
- What authentication methods are supported?
- I configured my SonicWALL SSL-VPN appliance to use Active Directory as the authentication method, but it fails with a very strange error message. Why?
- My Windows XPSP2 system cannot use the RDP-based connectors. Why?
- I created a FTP bookmark, but when I access it, the filenames are garbled – why?
- Where can I get a VNC client?
- Are the SSL-VPN 200/2000/4000 appliances fully supported by GMS or ViewPoint?
- Does the SonicWALL SSL-VPN appliance support printer mapping?
- Can I integrate SonicWALL SSL VPN with wireless?
- Can I manage the appliance on any interface IP address of the SonicWALL SSL-VPN appliance?
- Can I allow only certain Active Directory users access to log into the SonicWALL SSL-VPN appliance?
- Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)?
- Why are my RDP sessions dropping frequently?
- Can I create my own services for bookmarks rather than the services provided in the bookmarks section?
- Why can't I see all the servers on my network with the File Shares component?
- What port is the SSL-VPN appliance using for the Radius traffic?
- Do the SonicWALL SSL-VPN appliances support the ability for the same user account to login simultaneously?
- Does the SSL-VPN appliance support NT LAN Manager (NTLM) Authentication?
- I cannot connect to a web server when Windows Authentication is enabled. I get the following error message when I try that: 'It appears that the target web server is using an unsupported HTTP(S) authentication scheme through the SSL VPN, which currently supports only basic and digest authentication schemes. Please contact the administrator for further assistance.' - why?
- Why do Java Services, such as Telnet or SSH, not work through a proxy server?
- Why won't the SSH client connect to my SSH server?
- How are the F1-F12 keys handled in the Java-based SSHv1 and Telnet proxies?
- When I try to access a site that has Java applets using the SSL-VPN 200 all I see is a box with an 'x' in it -- why?
- There is no port option for the service bookmarks – what if these are on a different port than the default?
- What if I want a bookmark to point to a directory on a Web server?
- What versions of Citrix are supported?

Hardware FAQ

1. **What are the hardware specs for the SSL-VPN 200/2000/4000, SRA 1200 and SRA 4200?**

Answer:

Interfaces

SSL-VPN 200: (5) 10/100 Ethernet (WAN, 4-port LAN)

SSL-VPN 2000: (4) 10/100 Ethernet, (1) Serial port

SSL-VPN 4000: (6) 10/100 Ethernet, (1) Serial port

SRA 1200: (2) 10/100/1000 Ethernet, (1) RJ-45 Serial port (115200 Baud)

SRA 4200: (4) 10/100/1000 Ethernet, (1) RJ-45 Serial port (115200 Baud)

Processors

SSL-VPN 200: SonicWALL security processor, cryptographic accelerator

SSL-VPN 2000: 800 MHz x86 main processor, cryptographic accelerator

SSL-VPN 4000: P4 Celeron main processor, cryptographic accelerator

SRA 1200: 1.5 GHz Via C7 x86 processor

SRA 4200: 1.8 GHz Via C7 x86 processor, cryptographic accelerator

Memory (RAM)

SSL-VPN 200: 128 MB

SSL-VPN 2000: 512 MB

SSL-VPN 4000: 1 GB

SRA 1200: 1 GB

SRA 4200: 2 GB

Flash Memory

SSL-VPN 200: 16 MB

SSL-VPN 2000: 128 MB

SSL-VPN 4000: 128 MB

SRA 1200: 1 GB

SRA 4200: 1 GB

Power Supply

SSL-VPN 200: External 20W, 12VDC, 1.66A

SSL-VPN 2000: Internal

SSL-VPN 4000: Internal

SRA 1200: Internal

SRA 4200: Internal

Max Power Consumption

SSL-VPN 200: 10.4 W

SSL-VPN 2000: 48 W

SSL-VPN 4000: 108 W

SRA 1200: 53 W

SRA 4200: 75 W

Total Heat Dissipation

SSL-VPN 200: 35.6 BTU

SSL-VPN 2000: 163.7 BTU

SSL-VPN 4000: 368.3 BTU

SRA 1200: 181 BTU

SRA 4200: 256 BTU

Dimensions

SSL-VPN 200: 7.45 x 4.55 x 1.06 in (18.92 x 11.56 x 2.69 cm)

SSL-VPN 2000: 17.00 x 10.00 x 1.75 in (43.18 x 25.40 x 4.45 cm)

SSL-VPN 4000: 17.00 x 13.75 x 1.75 in (43.18 x 33.66 x 4.45 cm)

SRA 1200: 17.00 x 10.125 x 1.75 in (43.18 x 25.70 x 4.45 cm)

SRA 4200: 17.00 x 10.125 x 1.75 in (43.18 x 25.70 x 4.45 cm)

Weight

SSL-VPN 200: 1.25 lbs (0.57 kg)

SSL-VPN 2000: 8.50 lbs (3.86 kg)

SSL-VPN 4000: 13 lbs (8.39 kg)

SRA 1200: 9.5 lbs (4.31 kg)

SRA 4200: 8.70 lbs (3.95 kg)

Major Regulatory Compliance (all models)

SSL-VPN 200/2000/4000:

FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TUV/GS, CB

SRA 1200/4200:

FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TUV/GS, CB

WEEE, RoHS (Europe), RoHS (China)

FIPS: Mechanically Designed for FIPS 140-2 Level 2

Environment

Temperature:

SSL-VPN 200/2000/4000: 40-105ª F, 5-40ª C

SRA 1200/4200: 32-105ª F, 0-40ª C

Relative Humidity:

SSL-VPN 200/2000/4000: 10-90% non-condensing

SRA 1200/4200: 5-95% non-condensing

MTBF

SSL-VPN 200: 9.0 years

SSL-VPN 2000: 11.2 years

SSL-VPN 4000: 9.2 years

SRA 1200: 13 years

SRA 4200: 8.3 years

2. **Do the SSL-VPN appliances have hardware-based SSL acceleration onboard?**

Answer: All models except the SRA 1200 have hardware-based SSL accelerators onboard - even the SSL-VPN 200 model. The SRA 1200 does not have a hardware-based SSL accelerator processor.

3. **What are the main differences between the discontinued SonicWALL SSL-RX Accelerator from that of the SSL-VPN 200, 2000 and 4000 appliances?**

Answer: The discontinued SSL-RX Accelerator was a purpose-built appliance used to offload cryptographic processes from burdened servers. The SSL-VPN 200, 2000 & 4000 are designed to provide easy-to-use, lightweight, clientless access to internal network resources using a Web browser. The SSL-VPN 200 appliances cannot be used as an SSL Accelerator. The SSL-VPN 2000 & 4000, using Web Application Offloading in 3.5 can now function as an SSL Accelerator.

4. **What operating system do the SonicWALL SSL-VPN appliances run?**

Answer: The SonicWALL SSL-VPN appliance runs SonicWALL's own hardened Linux distribution.

5. **Can I put multiple SonicWALL SSL-VPN appliances behind a load-balancer?**

Answer: Yes, this should work fine as long as the load-balancer or content-switch is capable of tracking sessions based upon SSL Session ID persistence, or cookie-based persistence.

Table 23 SSL-VPN 200/2000/4000, SRA 1200/4200 Max Count Table

Type	Max Supported on 200	Max Supported on 2000	Max Supported on 4000	Max Supported on 1200	Max Supported on 4200
Portal entries	16	32	32	32	32
Domain entries	10	32	32	32	32
Group entries	32	64	64	64	64
User entries	100	1,000	2,000	1,000	1,000
NetExtender global client routes	32	32	32	50	50
NetExtender group client routes	N/A	12	12	50	50
NetExtender user client routes	N/A	12	12	50	50
Recommended concurrent users	10	50	200	25	50
Maximum concurrent users	50	512	1,024	50	512
Maximum concurrent Nx connections	30	125	300	50	125
Route entries	32	32	32	32	32

Type	Max Supported on 200	Max Supported on 2000	Max Supported on 4000	Max Supported on 1200	Max Supported on 4200
Host entries	32	32	32	32	32
Bookmark entries	32	32	32	300	300
Policy entries	12	12	12	32	32
Policy address entries	32	32	32	32	32
Network Objects	64	64	64	64	64
‘Address’ Network Objects	16	16	16	16	16
‘Network’ Network Objects	32	32	32	32	32
‘Service’ Network Objects	32	32	32	32	32
SMB shares	1,024	1,024	1,024	1,024	1,024
SMB nodes	1,024	1,024	1,024	1,024	1,024
SMB workgroups	8	8	8	8	8
Concurrent FTP sessions	8	8	8	8	8
Log size	250 KB	250 KB	250 KB	250 KB	250 KB

Table 24 Feature Support by Model, Firmware 2.1 and Newer

Feature	SSL-VPN 200	SSL-VPN 2000 SSL-VPN 4000 SRA 1200 SRA 4200
Seamless integration behind any firewall	X	X
Clientless connectivity	X	X
Unrestricted concurrent user tunnels	X	X
Enhanced layered security	X	X
NetExtender technology	X	X
Granular policy configuration controls	X	X
Personalized portal	X	X
File shares access policies	X	X
Standalone NetExtender client	X	X
RDP Java client	X	X
Context-sensitive help	X	X
Citrix (ICA) support		X
NetExtender: Support for multiple IP ranges and routes		X
Tokenless two-factor authentication	X	X
RSA support		X
Vasco support	X	X
Optional client certificate support		X
Graphical usage monitoring	X	X
Option to create system backup		X

Feature	SSL-VPN 200	SSL-VPN 2000 SSL-VPN 4000 SRA 1200 SRA 4200
OWA premium version and Lotus Domino Access		X
Single Sign-on bookmark policy options	X	X
Email log capability	X	X
Multiple RADIUS server support	X	X
RADIUS test function		X
NetExtender domain suffix support	X	X
SSHv2 support	X	X
Virtual Host/Domain Name support		X

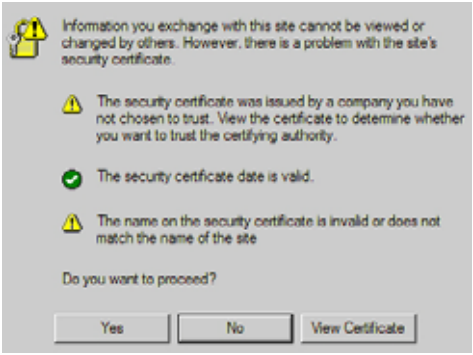
Digital Certificates and Certificate Authorities FAQ

1. What do I do if when I log in to the SonicWALL SSL-VPN appliance my browser gives me an error, or if my Java components give me an error?

Answer: These errors can be caused by any combination of the following three factors:

- The certificate in the SonicWALL SSL-VPN appliance is not trusted by the browser
- The certificate in the SonicWALL SSL-VPN appliance may be expired.
- The site requested by the client Web browser does not match the site name embedded in the certificate.

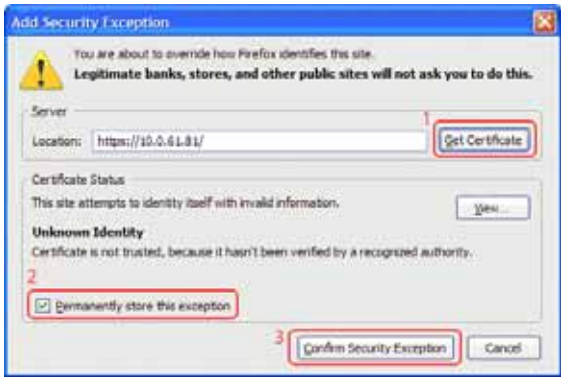
Web browsers are programmed to issue a warning if the above three conditions are not met precisely. This security mechanism is intended to ensure end-to-end security, but often confuses people into thinking something is broken. If you are using the default self-signed certificate, this error will appear every time a Web browser connects to the SonicWALL SSL-VPN appliance. However, it is just a warning and can be safely ignored, as it does not affect the security negotiated during the SSL handshake. If you do not want this error to happen, you will need to purchase and install a trusted SSL certificate onto the SonicWALL SSL-VPN appliance.



2. **I get this message below when I log into my SSL-VPN appliance using Firefox 3.0 – what do I do?**

Answer: Much like the errors shown above for Internet Explorer, Firefox 3.0 has a unique error message when any certificate problem is detected. The conditions for this error are the same as for the above Internet Explorer errors.

To get past this screen, click the **Or you can add an exception** link at the bottom, then click the **Add Exception** button that appears. In the Add Security Exception window that opens, click the **Get Certificate** button, ensure that **Permanently store this exception** is checked, and finally, click the **Confirm Security Exception** button. See below:

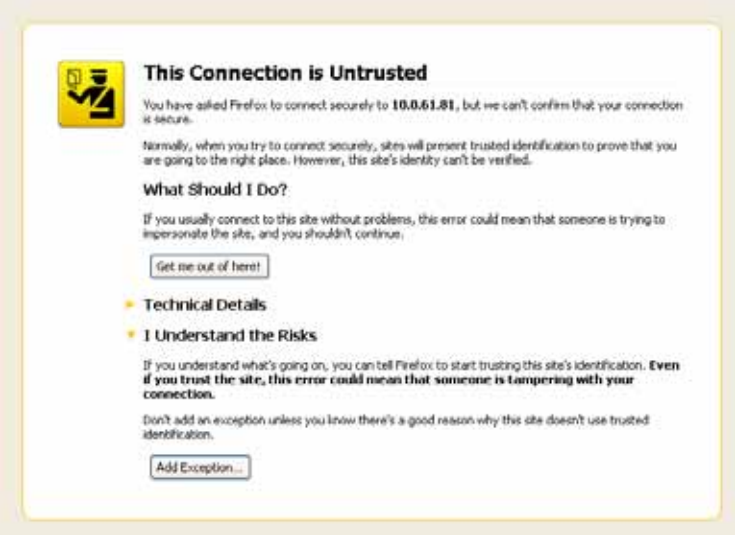


To avoid this inconvenience, it is strongly recommended that all SonicWALL SSL-VPN appliances, going forward, have a trusted digital certificate installed.

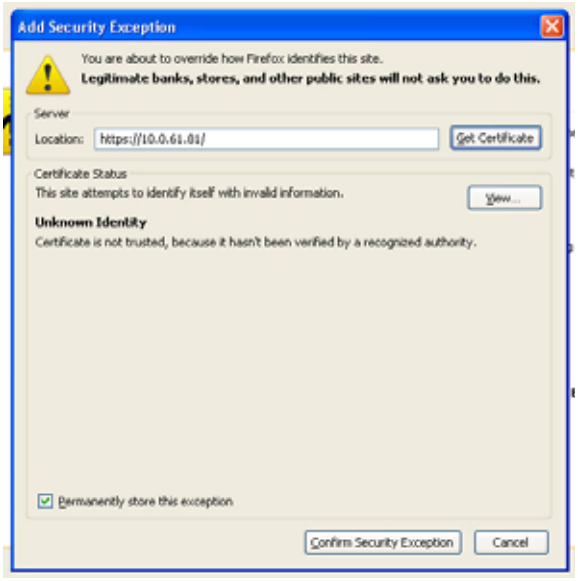
3. I get the warning below when I log into my SSL-VPN using Firefox 3.5 – what do I do?

Answer: This is the Firefox 3.5 warning message when any certificate problem is detected. The conditions for this error are the same as for the above Internet Explorer errors.

To get past this screen, click the arrow next to **I Understand the Risks** to expand the section, then click the **Add Exception** button that appears.



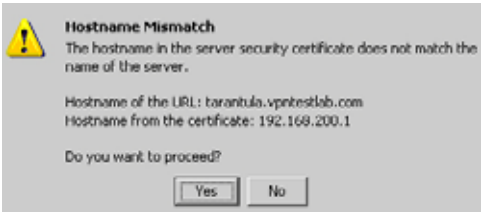
In the Add Security Exception window that opens, click the **Get Certificate** button, ensure that **Permanently store this exception** is checked, and finally, click the **Confirm Security Exception** button. See below:



To avoid this inconvenience, it is strongly recommended that all SonicWALL SSL-VPN appliances, going forward, have a trusted digital certificate installed.

4. **When I launch any of the Java components it gives me an error – what should I do?**

Answer: See the previous section. This occurs when the certificate is not trusted by the Web browser, or the site name requested by the browser does not match the name embedded in the site certificate presented by the SSL-VPN appliance during the SSL handshake process. This error can be safely ignored.



5. **Do I have to purchase a SSL certificate?**

Answer: No, you can simply ignore the security warnings, which are a message to users that the certificate is not trusted or contains mismatched information. Accepting a non-trusted certificate does not have anything to do with the level of encryption negotiated during the SSL handshake. However, SonicWALL tested digital certificates from www.rapidssl.com, which are inexpensive, work fine in the SonicWALL SSL-VPN appliance, and do not require the background check that other Certificate Authorities require during the purchase process. You can find a white paper on how to purchase and install a certificate online at: http://www.sonicwall.com/us/support/3165.html.

6. **What format is used for the digital certificates?**

Answer: X509v3.

7. **Are wild card certificates supported?**

Answer: Yes.

8. **What CA's certificates can I use with the SonicWALL SSL-VPN appliance?**

Answer: Any CA certificate should work if the certificate is in X509v3 format, including Verisign, Thawte, Baltimore, RSA, etc… To use Thawte certificates with the SSL-VPN appliances, you will need to upgrade to firmware 1.0.0.9 or newer.

9. **Does the SSL-VPN appliance support chained certificates?**

Answer: Yes, it does. On the System > Certificates page, do the following:

- Under "Server Certificates", click Import Certificate and upload the SSL server certificate and key together in a .zip file. The certificate should be named 'server.crt'. The private key should be named 'server.key'.
- Under "Additional CA Certificates", click Import Certificate button and upload the intermediate CA certificate(s). The certificate should be PEM encoded in a text file.

After uploading any intermediate CA certificates, the system should be restarted. The web server needs to be restarted with the new certificate included in the CA certificate bundle.

10. Any other tips when I purchase the certificate for the SSL-VPN appliance?

Answer: We recommend you purchase a multi-year certificate to avoid the hassle of renewing each year (most people forget and when the certificate expires it can create an administrative nightmare). It is also good practice to have all users that will connect to the SSL-VPN appliance run Windows Update (also known as Microsoft Update) and install the 'Root Certificates' update.

11. Can I use certificates generated from a Microsoft Certificate Server?

Answer: Yes, but to avoid a browser warning, you will need to install the Microsoft CA's root certificate into all Web browsers that will connect to the appliance.

12. Why can't I import my new certificate and private key?

Answer: Be sure that you upload a .zip file containing the PEM formatted private key file named "server.key" and the PEM formatted certificate file named "server.crt". The .zip file must have a flat file structure (no directories) and contain only "server.key" and "server.crt" files. The key and the certificate must also match, otherwise the import will fail.

13. Why do I see the status "pending" after importing a new certificate and private key?

Answer: Click the 'configure' icon next to the new certificate and enter the password you specified when creating the Certificate Signing Request (CSR) to finalize the import of the certificate. Once this is done, you can successfully activate the certificate on the SonicWALL SSL-VPN appliance.

14. Can I have more than one certificate active if I have multiple virtual hosts?

Answer: Prior to 2.5 firmware: No, only one can be active, other virtual sites with names that do not match the name embedded on the SSL-VPN appliance's certificate will show security warnings to any Web browser connecting to them.

With 2.5 firmware or later, it is possible to select a certificate for each Portal under the Portals > Portals: Edit Portal - Virtual Host tab. The portal Virtual Host Settings fields allow you to specify separate IP address, and certificate per portal. If the administrator has configured multiple portals, it is possible to associate a different certificate with each portal. For example, **sslvpn.test.sonicwall.com** might also be reached by pointing the browser to **virtualassist.test.sonicwall.com**. Each of those portal names can have its own certificate. This is useful to prevent the browser from displaying a certificate mismatch warning, such as "This server is abc, but the certificate is xyz, are you sure you want to continue?".

15. I imported the CSR into my CA's online registration site but it's asking me to tell them what kind of Webserver it's for. What do I do?

Answer: Select 'Apache'.

16. Can I store the key and certificate?

Answer: Yes, the key is exported with the CSR during the CSR generation process. It's strongly recommended that you can keep this in a safe place with the certificate you receive from the CA. This way, if the SonicWALL SSL-VPN appliance ever needs replacement or suffers a failure, you can reload the key and cert. You can also always export your settings from the System > Settings page.

17. Are PKCS#7 (chained certs) or PKCS#12 (key and cert PFX container) supported on the SSL-VPN appliance?

Answer: No, neither one is currently supported. SonicWALL is investigating supporting these in a future release.

18. Does the SonicWALL SSL-VPN appliance support client-side digital certificates?

Answer: Yes, client certificates are enforced per Domain or per User on the Users > Local Users: Edit User – Login Policies tab.

- Per Domain/Per User client certificate enforcement settings:
  - Option to Verify the user name matches the Common Name (CN) of the client certificate
  - Option to Verify partial DN in the client certificate subject (optional). The following variables are supported:

  User name: %USERNAME%

  Domain name: %USERDOMAIN%

  Active Directory user name: %ADUSERNAME%

  Wildcard: %WILDCARD%

Note Firmware prior to 3.5 required the client certificate CN field to be the username (CN=username) entered to login to the appliance.

- Support for Microsoft CA Subject Names where CN=<Full user name>, e.g. CN=John Doe. Client certificate authentication attempts for users in Active Directory domains will have the CN compared against the user's full name in AD.
- Detailed client certificate authentication failure messages and log messages are available in the Log > View page.
- Certificate Revocation List (CRL) Support. Each CA Certificate now supports an optional CRL via file import or periodic import via URL.

The client certificate must be loaded into the client's browser. Also, remember that any certificates in the trust chain of the client certificates must be installed onto the SSL-VPN appliance.

19. When client authentication is required my clients cannot connect even though a CA certificate has been loaded. Why?

Answer: After a CA certificate has been loaded, the SonicWALL SSL-VPN must be rebooted before it is used for client authentication. Failures to validate the client certificate will also cause failures to logon. Among the most common are certificate is not yet valid, certificate has expired, login name does not match common name of the certificate, certificate not sent.

NetExtender FAQ

1. Does NetExtender work on other operating systems than Windows?

Answer: Yes. Version 2.5 firmware added support for Mac and Linux platforms.

Mac Requirements:

- Mac OS X 10.5+
- Apple Java 1.6.0_10+ (can be installed/upgraded by going to Apple Menu > Software Update; should be pre-installed on OS X 10.5+)

Linux Requirements:

- i386-compatible distribution of Linux
- Sun Java 1.6.0_10+
- Fedora: FC3-FC10 have been tested successfully
- Suse: Tested successfully on 10.3
- Ubuntu: 8.04 works; 8.10 requires a NX 3.5.621 or higher

Separate NetExtender installation packages are also downloadable from mysonicwall.com for each release.

2. **Which versions of Windows does NetExtender support?**

Answer: NetExtender supports:

- Windows XP Service Pack 3 (SP3)
- Vista SP1
- Windows 7

3. **I tried to run NetExtender but it says I must have admin rights – why?**

Answer: If your SSL-VPN appliance is running 1.0 firmware, then on Windows 2000, XP, 2003, Vista, and Windows 7 systems the logged-in user must have administrative rights to be able to install ActiveX-based components such as NetExtender, and it will not be possible to run NetExtender on systems where you do not have administrative rights (this often is seen in kiosk or public computer environments, where the OS is locked down to prevent this sort of behavior). If your SSL-VPN appliance is running firmware 1.5 firmware or newer, a user can run NetExtender provided that a user with administrative rights previously installed NetExtender onto the system.

4. **Can I block communication between NetExtender clients?**

Answer: Yes, this can be achieved with the User/Group/Global Policies by adding a ‘deny’ policy for the NetExtender IP range.

5. **Can NetExtender run as a Windows service?**

Answer: The Windows version of NetExtender found in the 1.5 firmware release and newer can be installed and configured to run as a Windows service, which will allow systems to login to domains across the NetExtender client.

6. **What range do I use for NetExtender IP client address range?**

Answer: This range is the pool that incoming NetExtender clients will be assigned – NetExtender clients actually appear as though they are on the internal network – much like the Virtual Adapter capability found in SonicWALL’s Global VPN Client. You will need to dedicate one IP address for each active NetExtender session, so if you expect 20 simultaneous NetExtender sessions to be the maximum, create a range of 20 open IP addresses. Make sure that these IP addresses are open and are not used by other network appliances or contained within the scope of other DHCP servers. For example, if your SSL-VPN appliance is in one-port

mode on the X0 interface using the default IP address of 192.168.200.1, create a pool of addresses from 192.168.200.151 to 192.168.200.171. In the 1.5 firmware release, you can create multiple unique pools on a per-group or per-user basis.

7. **What do I enter for NetExtender client routes?**

Answer: These are the networks that will be sent to remote NetExtender clients and should contain all networks that you wish to give your NetExtender clients access to. For example, if your SonicWALL SSL-VPN appliance was in one-port mode, attached to a SonicWALL NSA 3500 appliance on a DMZ using 192.168.200.0/24 as the subnet for that DMZ, and the SonicWALL NSA 3500 had two LAN subnets of 192.168.168.0/24 and 192.168.170.0/24, you would enter those two LAN subnets as the client routes to provide NetExtender clients access to network resources on both of those LAN subnets.

8. **What does the 'Tunnel All Mode' option do?**

Answer: Activating this feature will cause the SonicWALL SSL-VPN appliance to push down two default routes that tell the active NetExtender client to send all traffic through the SonicWALL SSL-VPN appliance. This feature is useful in environments where the SonicWALL SSL-VPN appliance is deployed in tandem with a SonicWALL security appliance running all UTM services, as it will allow you to scan all incoming and outgoing NetExtender user traffic for viruses, spyware, intrusion attempts, and content filtering.

9. **Is there any way to see what routes the SonicWALL SSL-VPN is sending NetExtender?**

Answer: Yes, right-click on the NetExtender icon in the taskbar and select **route information**. You can also get status and connection information from this same menu.

10. **Once I install the NetExtender is it uninstalled when I leave my session?**

Answer: By default, when NetExtender is installed for the first time it stays resident on the system, although this can be controlled by selecting the **Uninstall On Browser Exit** > **Yes** option from the NetExtender icon in the taskbar while it is running. If this option is checked, NetExtender will remove itself when it is closed. It can also be uninstalled from the "Add/ Remove Program Files" in Control Panel. NetExtender remains on the system by default to speed up subsequent login times.

11. **How do I get new versions of NetExtender?**

Answer: New versions of NetExtender are included in each firmware release of the SSL-VPN software and have version control information contained within. If the SSL-VPN appliance has been upgraded with new software, and a connection is made from a system using a previous, older version of NetExtender, it will automatically be upgraded to the new version.

There is one exception to the automatic upgrading feature: it is not supported for the MSI version of NetExtender. If NetExtender was installed with the MSI package, it must be upgraded with a new MSI package. The MSI package is designed for the administrator to deploy NetExtender through Active Directory, allowing full version control through Active Directory.

12. **How is NetExtender different from a traditional IPSec VPN client, such as SonicWALL's Global VPN Client (GVC)?**

Answer: NetExtender is designed as an extremely lightweight client that is installed via a Web browser connection, and utilizes the security transforms of the browser to create a secure, encrypted tunnel between the client and the SonicWALL SSL-VPN appliance.

13. **Is NetExtender encrypted?**

Answer: Yes, it uses whatever cipher the NetExtender client and SSL-VPN appliance negotiate during the SSL connection.

14. **Is there a way to secure clear text traffic between the SonicWALL SSL-VPN appliance and the server?**

Answer: Yes, you can configure the Microsoft Terminal Server to use encrypted RDP-based sessions, and use HTTPS reverse proxy.

15. What is the PPP adapter that is installed when I use the NetExtender?

Answer: This is the transport method NetExtender uses. It also uses compression (MPPC). You can elect to have it removed during disconnection by selecting this from the NetExtender menu.

16. What are the advantages of using the NetExtender instead of a Proxy Application?

Answer: NetExtender allows full connectivity over an encrypted, compressed PPP connection allowing the user to directly to connect to internal network resources. For example, a remote user could launch NetExtender to directly connect to file shares on a corporate network.

17. Does performance change when using NetExtender instead of proxy?

Answer: Yes. NetExtender connections put minimal load on the SonicWALL SSL-VPN appliances, whereas many proxy-based connections may put substantial strain on the SonicWALL SSL-VPN appliance. Note that HTTP proxy connections use compression to reduce the load and increase performance. Content received by the SSL-VPN from the local Web server is compressed using gzip before sending it over the Internet to the remote client. Compressing content sent from the SSL-VPN saves bandwidth and results in higher throughput. Furthermore, only compressed content is cached, saving nearly 40-50% of the required memory. Note that gzip compression is not available on the local (clear text side) of the SSL-VPN appliance, or for HTTPS requests from the remote client.

18. SonicWALL SSL VPN is application dependent; how can I address non-standard applications?

Answer: You can use NetExtender to provide access for any application that cannot be accessed using internal proxy mechanisms - HTTP, HTTPS, FTP, RDP4 (firmware 1.0 only), ActiveX-based RDP, Java-based RDP (firmware 1.5 and newer), Telnet, and SSHv1. With 3.5 firmware and later, Application Offloading can be used for web applications. In this way, the SSL-VPN functions similar to an SSL offloader and will proxy web applications pages without the need for URL rewriting.

19. Speaking of SSH, is SSHv2 supported?

Answer: Yes, this is supported in firmware 2.0 and newer.

20. Why is it required that an ActiveX component be installed?

Answer: NetExtender is installed via an ActiveX-based plug-in from Internet Explorer. Users using Firefox browsers may install NetExtender via an XPI installer. NetExtender may also be installed via an MSI installer. Download the NetExtender MSI installer from mysonicwall.com.

21. Does NetExtender support desktop security enforcement, such as AV signature file checking, or Windows registry checking?

Answer: Not at present, although these sorts of features are planned for future releases of NetExtender.

22. Does NetExtender work with the 64-bit version of Microsoft Windows?

Answer: Yes, starting with 3.0 firmware, NetExtender supports 64-bit Windows 7, Vista and XP.

23. Does NetExtender work 32-bit and 64-bit version of Microsoft Windows 7?

Answer: Yes, starting with 3.0.0.9-20sv and later firmware, NetExtender supports 32-bit and 64-bit Windows 7.

24. Does NetExtender support client-side certificates?

Answer: Yes, in 3.5 and up the Windows NetExtender client supports client certificate authentication from the stand-alone client. Users can also authenticate to the SSL-VPN portal and then launch NetExtender.

25. **My firewall is dropping NetExtender connections from my SonicWALL SSL-VPN as being spoofs. Why?**

Answer: If the NetExtender addresses are on a different subnet than the X0 interface, a rule needs to be created for the firewall to know that these addresses are coming from the SonicWALL SSL-VPN.

General FAQ

1. **Is the SonicWALL SSL-VPN appliance a true reverse proxy?**

Answer: Yes, the HTTP, HTTPS, CIFS, FTP are Web-based proxies, where the native Web browser is the client. VNC, RDP - ActiveX, RDP - Java, SSHv1 and Telnet use browser-delivered Java or ActiveX clients. NetExtender on Windows uses a browser-delivered client.

2. **What browser and version do I need to successfully connect to the SonicWALL SSL-VPN appliance?**

Answer:

- Microsoft Internet Explorer 8.0 or newer
- Mozilla Firefox 11.0 or newer
- Google Chrome 18.0 or newer

3. **What needs to be activated on the browser for me to successfully connect to the SonicWALL SSL-VPN appliance?**

Answer:

- SSLv2, SSLv3, or TLS – recommend disabling SSLv2 if possible
- Enable cookies
- Enable pop-ups for the site
- Enable Java
- Enable Javascript
- Enable ActiveX

4. **What version of Java do I need?**

Answer: You will need to install SUN's JRE 1.6.0_10 or higher (available at http://www.java.com) to use some of the features on the SonicWALL SSL-VPN appliance. On Google Chrome, you will need Java 1.6.0 update 10 or higher.

5. **What operating systems are supported?**

Answer:

- Microsoft Windows 2000 Professional SP4 and newer
- Microsoft XP, SP2 and newer
- Microsoft Vista
- Microsoft Windows 7
- Apple OSX 10.5 and newer
- Linux kernel 2.4.x and newer

6. **Why does the 'File Shares' component not recognize my server names?**

Answer: If you cannot reach your server by its NetBIOS name, there might be a problem with name resolution. Check your DNS and WINS settings on the SonicWALL SSL-VPN appliance. You might also try manually specifying the NetBIOS name to IP mapping in the "Network > Host Resolution" section, or you could manually specify the IP address in the UNC path, e.g. \\192.168.100.100\sharefolder.

Also, if you get an authentication loop or an error, is this File Share a DFS server on a Windows domain root? When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SonicWALL SSL-VPN is not a domain member and will not be able to connect to the DFS shares.DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

7. **Does the SonicWALL SSL-VPN appliance have a SPI firewall?**

Answer: No. It must be combined with a SonicWALL security appliance or other third-party firewall/VPN device.

8. **Can I access the SonicWALL SSL-VPN appliance using HTTP?**

Answer: No, it requires HTTPS. HTTP connections are immediately redirected to HTTPS. You may wish to open both 80 and 443, as many people forget to type https: and instead type http://. If you block 80, it will not get redirected.

9. **What is the most common deployment of the SonicWALL SSL-VPN appliances?**

Answer: One-port mode, where only the X0 interface is utilized, and the appliance is placed in a separated, protected “DMZ” network/interface of a SonicWALL security appliance, such as the SonicWALL TZ 180, or the SonicWALL NSA appliance.

10. **Why is it recommended to install the SonicWALL SSL-VPN appliance in one-port mode with a SonicWALL security appliance?**

Answer: This method of deployment offers additional layers of security control plus the ability to use SonicWALL’s Unified Threat Management (UTM) services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering and Intrusion Prevention, to scan all incoming and outgoing NetExtender traffic.

11. **Is there an installation scenario where you would use more than one interface or install the appliance in two-port mode?**

Answer: Yes, when it would be necessary to bypass a firewall/VPN device that may not have an available third interface, or a device where integrating the SonicWALL SSL-VPN appliance may be difficult or impossible.

12. **Can I cascade multiple SonicWALL SSL-VPN appliances to support more concurrent connections?**

Answer: No, this is not supported.

13. **Why can’t I log into the management interface of the SonicWALL SSL-VPN?**

Answer: The default IP address of the appliance is 192.168.200.1 on the X0 interface. If you cannot reach the appliance, try cross-connecting a system to the X0 port, assigning it a temporary IP address of 192.168.200.100, and attempt to log into the SonicWALL SSL-VPN appliance at https://192.168.200.1. Then verify that you have correctly configured the DNS and default route settings on the Network pages.

14. **Can I create site-to-site VPN tunnels with the SonicWALL SSL-VPN appliance?**

Answer: No, it is only a client-access appliance. If you require this, you will need a SonicWALL TZ-series or NSA security appliance.

15. **Can the SonicWALL Global VPN Client (or any other third-party VPN client) connect to the SonicWALL SSL-VPN appliance?**

Answer: No, only NetExtender and proxy sessions are supported.

16. **Can I connect to the SonicWALL SSL-VPN appliance over a modem connection?**

Answer: Yes, although performance will be slow, even over a 56K connection it is usable.

17. What SSL ciphers are supported by the SSL-VPN appliance?

Answer: Starting with 3.5 firmware, SonicWALL only uses HIGH security ciphers with SSLv3 and TLSv1:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5

18. Is AES supported in SonicWALL SSL VPN?

Answer: Yes, if your browser supports it.

19. Can I expect similar performance (speed, latency, and throughput) as my IPSec VPN?

Answer: Yes, actually you may see better performance as NetExtender uses multiplexed PPP connections and runs compression over the connections to improve performance.

20. Is 2-factor authentication (RSA SecurID, etc) supported?

Answer: Yes, this is supported in the 2.0 firmware release and newer. This feature is only supported on the 2000 and 4000 platforms. It will not be supported on the 200 platform.

21. Does the SonicWALL SSL-VPN appliance support VoIP?

Answer: Yes, over NetExtender connections.

22. Is Syslog supported?

Answer: Yes.

23. Does NetExtender support multicast?

Answer: Not at this time. Look for this in a future firmware release.

24. Are SNMP and Syslog supported?

Answer: Syslog forwarding to up to two external servers is supported in the current software release. SNMP is not currently supported but may be planned for a future software release.

25. Does the SonicWALL SSL-VPN appliance have a Command Line Interface (CLI)?

Answer: No, it does not. The console ports on the SSL-VPN 2000 and SSL-VPN 4000 appliances are disabled and cannot be accessed. The SSL-VPN 200 appliance does not have a console port.

26. Can I Telnet or SSH into the SSL-VPN appliance?

Answer: No, neither Telnet or SSH are supported in the current release of the SSL-VPN appliance software as a means of management (this is not to be confused with the Telnet and SSH proxies, which the appliance does support).

27. When controlling user access, can I apply permissions on both a domain as well as a Forest basis?

Answer: Yes, using the LDAP connector.

28. What does the Web cache cleaner do?

Answer: The Web cache cleaner is an ActiveX-based applet that removes all temporary files generated during the session, removes any history bookmarks, and removes all cookies generated during the session. It will only run on Internet Explorer 8.0 or newer.

29. Why didn't the Web cache cleaner work when I exited the Web browser?

Answer: In order for the Web cache cleaner to run, you must click on the **Logout** button. If you close the Web browser using any other means, the Web cache cleaner cannot run.

30. What does the 'encrypt settings file' checkbox do?

Answer: This setting will encrypt the settings file so that if it is exported it cannot be read by unauthorized sources. Although it is encrypted, it can be loaded back onto the SonicWALL SSL-VPN appliance (or a replacement appliance) and decrypted. If this box is not selected, the exported settings file is clear-text and can be read by anyone.

31. What does the 'store settings' button do?

Answer: By default, the settings are automatically stored on a SSL-VPN 2000 and SSL-VPN 4000 appliance any time a change to programming is made, but this can be shut off if desired. If this is disabled, all unsaved changes to the appliance will be lost. This feature is most useful when you are unsure of making a change that may result in the box locking up or dropping off the network. If the setting is not immediately saved, you can power-cycle the box and it will return to the previous state before the change was made.

32. What does the 'create backup' button do?

Answer: This feature allows you to create a backup snapshot of the firmware and settings into a special file that can be reverted to from the management interface or from SafeMode. SonicWALL strongly recommends creating system backup right before loading new software, or making significant changes to the programming of the appliance. This feature is available only on the SonicWALL SSL-VPN 2000 and SSL-VPN 4000 appliances.

33. What is 'SafeMode'?

Answer: SafeMode is a feature of the SonicWALL SSL-VPN appliance that allows administrators to switch between software image builds and revert to older versions in case a new software image turns out to cause issues. In cases of software image corruption, the appliance will boot into a special interface mode that allows the administrator to choose which version to boot, or load a new version of the software image.

34. How do I access the SafeMode menu?

Answer: In emergency situations, you can access the SafeMode menu by holding in the Reset button on the SSL-VPN appliance (the small pinhole button located on the front of the SSL-VPN 2000 or SSL-VPN 4000, and on the back of the SSL-VPN 200) for 12-14 seconds until the 'Test' LED begins quickly flashing yellow. Once the SonicWALL has booted into the SafeMode menu, assign a workstation a temporary IP address in the 192.168.200.x subnet, such as 192.168.200.100, and attach it to the X0 interface on the SSL-VPN appliance. Then, using a modern Web browser (Microsoft IE6.x+, Mozilla 1.4+), access the special SafeMode GUI using the appliance's default IP address of 192.168.200.1. You will be able to boot the appliance using a previously saved backup snapshot, or you can upload a new version of software with the **Upload New Software image** button.

35. Can I change the colors of the portal pages?

Answer: This is not supported in the current releases, but is planned for a future software release.

36. What authentication methods are supported?

Answer: Local database, RADIUS, Active Directory, NT4, and LDAP.

37. I configured my SonicWALL SSL-VPN appliance to use Active Directory as the authentication method, but it fails with a very strange error message. Why?

Answer: The appliances must be precisely time-synchronized with each other or the authentication process will fail. Ensure that the SonicWALL SSL-VPN appliance and the Active Directory server are both using NTP to keep their internal clocks synchronized.

38. My Windows XPSP2 system cannot use the RDP-based connectors. Why?

Answer: You will need to download and install a patch from Microsoft for this to work correctly. The patch can be found at the following site: http://www.microsoft.com/downloads/details.aspx?FamilyID=17d997d2-5034-4bbb-b74dad8430a1f7c8&DisplayLang=en. You will need to reboot your system after installing the patch.

39. I created a FTP bookmark, but when I access it, the filenames are garbled – why?

Answer: If you are using a Windows-based FTP server, you will need to change the directory listing style to 'UNIX' instead of 'MS-DOS'.

40. Where can I get a VNC client?

Answer: SonicWALL has done extensive testing with RealVNC. It can be downloaded at:

http://www.realvnc.com/download.html

41. Are the SSL-VPN 200/2000/4000 appliances fully supported by GMS or ViewPoint?

Answer: You need SonicOS SSL VPN 1.5.0.3 or higher for basic management by SonicWALL GMS; SonicOS SSL VPN 2.1 or higher is required for SSL VPN Reporting in SonicWALL GMS or ViewPoint.

42. Does the SonicWALL SSL-VPN appliance support printer mapping?

Answer: Yes, this is supported with the ActiveX-based RDP client only. The Microsoft Terminal Server RDP connector must be enabled first for this to work. You may need to install the correct printer driver software on the Terminal Server you are accessing.

43. Can I integrate SonicWALL SSL VPN with wireless?

Answer: Yes, refer to: http://www.sonicwall.com/support/pdfs/swisg.pdf

44. Can I manage the appliance on any interface IP address of the SonicWALL SSL-VPN appliance?

Answer: Prior to 2.5 firmware: No, the appliance can only by managed using the X0's IP address. With 2.5 firmware and later, yes, you can manage on any of the interface IP addresses.

45. Can I allow only certain Active Directory users access to log into the SonicWALL SSL-VPN appliance?

Answer: Yes. On the Users > Local Groups page, edit a group belonging to the Active Directory domain used for authentication and add one or more AD Groups under the **AD Groups** tab.

46. Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)?

Answer: Yes, but this is supported on SSL-VPN 2000 and SSL-VPN 4000 appliances only.

47. Why are my RDP sessions dropping frequently?

Answer: Try adjusting the session and connection timeouts on both the SSL-VPN appliance and any appliance that sits between the endpoint client and the destination server. If the SSL-VPN appliance is behind a firewall, adjust the TCP timeout upwards and enable fragmentation.

48. Can I create my own services for bookmarks rather than the services provided in the bookmarks section?

Answer: This is not supported in the current release of software but may be supported in a future software release.

49. Why can't I see all the servers on my network with the File Shares component?

Answer: The CIFS browsing protocol is limited by the server's buffer size for browse lists. These browse lists contain the names of the hosts in a workgroup or the shares exported by a host. The buffer size depends on the server software. Windows personal firewall has been known to cause some issues with file sharing even when it is stated to allow such access. If possible, try disabling such software on either side and then test again.

50. What port is the SSL-VPN appliance using for the Radius traffic?

Answer: It uses port 1812.

51. Do the SonicWALL SSL-VPN appliances support the ability for the same user account to login simultaneously?

Answer: Yes, this is supported on 1.5 and newer firmware releases. On the portal layout, you can enable or disable 'Enforce login uniqueness' option. If this box is unchecked, users can log in simultaneously with the same username and password.

52. Does the SSL-VPN appliance support NT LAN Manager (NTLM) Authentication?

Answer: Yes, in SSL VPN 4.0 and later releases, backend Web servers using NTLM or Windows Integrated Authentication are supported. Single Sign-On with NTLM is also supported. NTLM support is specific to Application Offloading and/or reverse-proxy bookmarks.

SSL VPN 3.5 and earlier do not support NTLM authentication. As a work around, the administrator can turn on basic or digest authentication. Basic authentication specifies the username and password in clear text, but the security outside the intranet is not compromised because the SSL-VPN uses HTTPS. However, the intranet is required to be "trusted". Digest authentication works better in this case, because the password is not sent in clear text and only a MD5 checksum that incorporates the password is sent.

53. I cannot connect to a web server when Windows Authentication is enabled. I get the following error message when I try that: 'It appears that the target web server is using an unsupported HTTP(S) authentication scheme through the SSL VPN, which currently supports only basic and digest authentication schemes. Please contact the administrator for further assistance.' - why?

Answer: In SSL VPN 3.5 and earlier releases, the HTTP proxy does not support Windows Authentication (formerly called NTLM). Only anonymous or basic authentication is supported.

54. Why do Java Services, such as Telnet or SSH, not work through a proxy server?

Answer: When the Java Service is started it does not use the proxy server. Transactions are done directly to the SSL-VPN.

55. Why won't the SSH client connect to my SSH server?

Answer: Check the version of SSH you have enabled on your server, and check the firmware release on the SSL-VPN appliance. SSHv2 support was not added until firmware 2.0 and newer. It's possible that there is a mismatch between the two.

56. How are the F1-F12 keys handled in the Java-based SSHv1 and Telnet proxies?

Answer: The Telnet server must support function keys. If it does, the keyboard used is relevant. Currently, the Telnet proxy uses vt320 and the SSHv1 proxy uses vt100 key codes. This is the default and the SSL-VPN appliance does not support other types such as SCO-ANSI yet. This may be supported in a future firmware release.

57. When I try to access a site that has Java applets using the SSL-VPN 200 all I see is a box with an 'x' in it -- why?

Answer: Proxying of Java applets through the reverse proxy is not supported on the SSL-VPN 200 platform.

58. There is no port option for the service bookmarks – what if these are on a different port than the default?

Answer: You can specify in the IP address box an 'IPaddress:portid' pair for HTTP, HTTPS, Telnet, Java, and VNC.

59. What if I want a bookmark to point to a directory on a Web server?

Answer: Add the path in the IP address box: IP/mydirectory/.

When I access Microsoft Telnet Server using a telnet bookmark it does not allow me to enter a user name -- why?

Answer: This is not currently supported on the appliance.

60. What versions of Citrix are supported?

Answer: Citrix Portal Bookmarks have been tested and verified to support the following Citrix Application Virtualization platforms through the Citrix Web Interface:

- Servers: Citrix XenApp 5.0, XenApp 4.5, XenApp/Presentation Server 4.5, Presentation Server 4.0 and MetaframeXP Feature Release 3
- Clients: XenApp Plugin version 11.0 or earlier versions and Java client version 9.6 or earlier versions

Appendix F: Glossary

Active Directory (AD) -. A centralized directory service system produced by Microsoft that automates network management of user data, security and resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

Common Internet File System (CIFS)

File Shares: SonicWALL's network file browsing feature on the SSL-VPN. This uses the Web browser to browse shared files on the network.

Lightweight Directory Access Protocol (LDAP) - An Internet protocol that email and other programs use to retrieve data from a server.

One-time Password (One-time Password) - A randomly-generated, single-use password. One-time Password may be used to refer to a particular instance of a password, or to the feature as a whole.

Simple Mail Transfer Protocol (SMTP) - A protocol for sending email messages between servers.

Secure Socket Layer Virtual Private Network (SSL VPN) - A remote access tool that utilizes a Web browser to provide clientless access to private applications.

Virtual Office - The user interface of SonicWALL SSL-VPN.

Windows Internet Naming Service (WINS) - A system that determines the IP address associated with a network computer.

Appendix G: SMS Email Formats

This section provides a list of SMS (Short Message Service) formats for worldwide cellular carriers. Find the correct format for your carrier from the list below, using your own phone number before the @ sign.

Note These SMS email formats are for reference only. These email formats are subject to change and may vary. You may 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.

Carrier	SMS Format
3River Wireless	4085551212@sms.3rivers.net
AirTel	4085551212@@airtelmail.com
AT&T Wireless	4085551212@mobile.att.net
Andhra Pradesh Airtel	4085551212@airtelap.com
Andhra Pradesh Idea Cellular	4085551212@ideacellular.net
Alltel PC	4085551212@message.alltel.com
Alltel	4085551212@alltelmessage.com
Arch Wireless	4085551212@archwireless.net
BeeLine GSM	4085551212@sms.beemail.ru
BeeLine (Moscow)	4085551212@sms.gate.ru
Bell Canada	4085551212@txt.bellmobility.ca
Bell Canada	4085551212@bellmobility.ca
Bell Atlantic	4085551212@message.bam.com
Bell South	4085551212@sms.bellsouth.com
Bell South	4085551212@wireless.bellsouth.com
Bell South	4085551212@blsdcs.net
Bite GSM (Lithuania)	4085551212@sms.bite.lt
Bluegrass Cellular	4085551212@sms.bluecell.com
BPL mobile	4085551212@bplmobile.com
Celcom (Malaysia)	4085551212@sms.celcom.com.my
Cellular One	4085551212@mobile.celloneusa.com

Carrier	SMS Format
Cellular One East Cost	4085551212@phone.cellone.net
Cellular One South West	4085551212@swmsg.com
Cellular One	4085551212@mobile.celloneusa.com
Cellular One	4085551212@cellularone.txtmsg.com
Cellular One	4085551212@cellularone.textmsg.com
Cellular South	4085551212@csouth1.com
CenturyTel	4085551212@messaging.centurytel.net
Cingular	4085551212@mobile.mycingular.net
Cingular Wireless	4085551212@mycingular.textmsg.com
Comcast	4085551212@comcastpcs.textmsg.com
CZECH EuroTel	4085551212@sms.eurotel.cz
CZECH Paegas	4085551212@sms.paegas.cz
Chennai Skycell / Airtel	4085551212@airtelchennai.com
Chennai RPG Cellular	4085551212@rpgmail.net
Comviq GSM Sweden	4085551212@sms.comviq.se
Corr Wireless Communications	4085551212@corrwireless.net
D1 De TeMobil	4085551212@t-d1-sms.de
D2 Mannesmann Mobilefunk	4085551212@d2-message.de
DT T-Mobile	4085551212@t-mobile-sms.de
Delhi Airtel	4085551212@airtelmail.com
Delhi Hutch	4085551212@delhi.hutch.co.in
Dobson-Cellular One	4085551212@mobile.cellularone.com
Dobson Cellular Systems	4085551212@mobile.dobson.net
Edge Wireless	4085551212@sms.edgewireless.com
E-Plus (Germany)	4085551212 @eplus.de
EMT	4085551212@sms.emt.ee
Eurotel (Czech Republic)	4085551212@sms.eurotel.cz
Europolitan Sweden	4085551212@europolitan.se
Escotel	4085551212@escotelmobile.com
Estonia EMT	4085551212@sms-m.emt.ee
Estonia RLE	4085551212@rle.ee
Estonia Q GSM	4085551212@qgsm.ee
Estonia Mobil Telephone	4085551212@sms.emt.ee
Fido	4085551212@fido.ca
Georgea geocell	4085551212@sms.ge
Goa BPLMobil	4085551212@bplmobile.com
Golden Telecom	4085551212@sms.goldentele.com
Golden Telecom (Kiev, Ukraine only)	4085551212@sms.gt.kiev.ua
GTE	4085551212@messagealert.com

Carrier	SMS Format
GTE	4085551212@airmessage.net
Gujarat Idea	4085551212@ideacellular.net
Gujarat Airtel	4085551212@airtelmail.com
Gujarat Celforce / Fascel	4085551212@celforce.com
Goa Airtel	4085551212@airtelmail.com
Goa BPLMobil	4085551212@bplmobile.com
Goa Idea Cellular	4085551212@ideacellular.net
Haryana Airtel	4085551212@airtelmail.com
Haryana Escotel	4085551212@escotelmobile.com
Himachal Pradesh Airtel	4085551212@airtelmail.com
Houston Cellular	4085551212@text.houstoncellular.net
Hungary Pannon GSM	4085551212@sms.pgsm.hu
Idea Cellular	4085551212@ideacellular.net
Inland Cellular Telephone	4085551212@inlandlink.com
Israel Orange IL	4085551212- @shiny.co.il
Karnataka Airtel	4085551212@airtelkk.com
Kerala Airtel	4085551212@airtelmail.com
Kerala Escotel	4085551212@escotelmobile.com
Kerala BPL Mobile	4085551212@bplmobile.com
Kyivstar (Kiev Ukraine only)	4085551212@sms.kyivstar.net
Kyivstar	4085551212@smsmail.lmt.lv
Kolkata Airtel	4085551212@airtelkol.com
Latvia Baltcom GSM	4085551212@sms.baltcom.lv
Latvia TELE2	4085551212@sms.tele2.lv
LMT	4085551212@smsmail.lmt.lv
Madhya Pradesh Airtel	4085551212@airtelmail.com
Maharashtra Idea Cellular	4085551212@ideacellular.net
MCI Phone	408555121 @mci.com
Meteor	4085551212@mymeteor.ie
Metro PCS	4085551212@mymetropcs.com
Metro PCS	4085551212@metorpcs.sms.us
MiWorld	4085551212@m1.com.sg
Mobileone	4085551212@m1.com.sg
Mobilecomm	4085551212@mobilecomm.net
Mobtel	4085551212@mobtel.co.yu
Mobitel (Tanazania)	4085551212@sms.co.tz
Mobistar Belgium	4085551212@mobistar.be
Mobility Bermuda	4085551212@ml.bm
Movistar (Spain)	4085551212@correo.movistar.net

Carrier	SMS Format
Maharashtra Airtel	4085551212@airtelmail.com
Maharashtra BPL Mobile	4085551212@bplmobile.com
Manitoba Telecom Systems	4085551212@text.mtsmobility.
Mumbai Orange	4085551212@orangemail.co.in
MTS (Russia)	4085551212@sms.mts.ru
MTC	4085551212@sms.mts.ru
Mumbai BPL Mobile	4085551212@bplmobile.com
MTN (South Africa only)	4085551212@sms.co.za
MiWorld (Singapore)	4085551212@m1.com.sg
NBTel	4085551212@wirefree.informe.ca
Netcom GSM (Norway)	4085551212@sms.netcom.no
Nextel	4085551212@messaging.nextel.com
Nextel	4085551212@nextel.com.br
NPI Wireless	4085551212@npiwireless.com
Ntelos	4085551212number@pcs.ntelos.com
One Connect Austria	4085551212@onemail.at
OnlineBeep	4085551212@onlinebeep.net
Omnipoint	4085551212@omnipointpcs.com
Optimus (Portugal)	4085551212@sms.optimus.pt
Orange - NL / Dutchtone	4085551212@sms.orange.nl
Orange	4085551212@orange.net
Oskar	4085551212@mujoskar.cz
Pacific Bell	4085551212@pacbellpcs.net
PCS One	4085551212@pcsone.net
Pioneer / Enid Cellular	4085551212@msg.pioneerenidcellular.com
PlusGSM (Poland only)	4085551212@text.plusgsm.pl
P&T Luxembourg	4085551212@sms.luxgsm.lu
Poland PLUS GSM	4085551212@text.plusgsm.pl
Primco	4085551212@primeco@textmsg.com
Primtel	4085551212@sms.primtel.ru
Public Service Cellular	4085551212@sms.pscel.com
Punjab Airtel	4085551212@airtelmail.com
Qwest	4085551212@qwestmp.com
Riga LMT	4085551212@smsmail.lmt.lv
Rogers AT&T Wireless	4085551212@pcs.rogers.com
Safaricom	4085551212@safaricomsms.com
Satelindo GSM	4085551212@satelindogsm.com
Simobile (Slovenia)	4085551212@simobil.net
Sunrise Mobile	4085551212@mysunrise.ch

Carrier	SMS Format
Sunrise Mobile	4085551212@freesurf.ch
SFR France	4085551212@sfr.fr
SCS-900	4085551212@scs-900.ru
Southwestern Bell	4085551212@email.swbw.com
Sonofon Denmark	4085551212@note.sonofon.dk
Sprint PCS	4085551212@messaging.sprintpcs.com
Sprint	4085551212@sprintpaging.com
Swisscom	4085551212@bluewin.ch
Swisscom	4085551212@bluemail.ch
Telecom Italia Mobile (Italy)	4085551212@posta.tim.it
Telenor Mobil Norway	4085551212@mobilpost.com
Telecel (Portugal)	4085551212@sms.telecel.pt
Tele2	4085551212@sms.tele2.lv
Tele Danmark Mobil	4085551212@sms.tdk.dk
Telus	4085551212@msg.telus.com
Telenor	4085551212@mobilpost.no
Telia Denmark	4085551212@gsm1800.telia.dk
TIM	4085551212 @timnet.com
TMN (Portugal)	4085551212@mail.tmn.pt
T-Mobile Austria	4085551212@sms.t-mobile.at
T-Mobile Germany	4085551212@t-d1-sms.de
T-Mobile UK	4085551212@t-mobile.uk.net
T-Mobile USA	4085551212@tmomail.net
Triton	4085551212@tms.suncom.com
Tamil Nadu Aircel	4085551212@airsms.com
Tamil Nadu BPL Mobile	4085551212 @bplmobile.com
UMC GSM	4085551212@sms.umc.com.ua
Unicel	4085551212@utext.com
Uraltel	4085551212@sms.uraltel.ru
US Cellular	4085551212@email.uscc.net
US West	4085551212@uswestdatamail.com
Uttar Pradesh (West) Escotel	4085551212@escotelmobile.com
Verizon	4085551212@vtext.com
Verizon PCS	4085551212@myvzw.com
Virgin Mobile	4085551212@vmobl.com
Vodafone Omnitel (Italy)	4085551212@vizzavi.it
Vodafone Italy	4085551212@sms.vodafone.it
Vodafone Japan	4085551212@pc.vodafone.ne.j
Vodafone Japan	4085551212@h.vodafone.ne.jp

Carrier	SMS Format
Vodafone Japan	4085551212@t.vodafone.ne.jp
Vodafone Spain	4085551212@vodafone.es
Vodafone UK	4085551212@vodafone.net
West Central Wireless	4085551212@sms.wcc.net
Western Wireless	4085551212@cellularonewest.com

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

PN: 232-001840-00
Rev D 6/12